Information Security FUNDAMENTALS

Second Edition

Thomas R. Peltier

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Information Security FUNDAMENTALS

Second Edition

Information Security FUNDAMENTALS

Second Edition

Thomas R. Peltier

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20130626

International Standard Book Number-13: 978-1-4398-1063-7 (eBook - PDF)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To the souls that left us too early: Justin Peltier, Gene Schultz,
and Brad Smith. They were always eager to try new things first—
I know they will make our next meeting a joyous occasion.

Contents

Acknowledgments

This book is the combined effort of many industry professionals. This group includes John Blackley, Maria Dailey, Pat Howard, Charles Johnson, Kimberly Logan, Kevin McLaughlin, John O'Leary, Justin Peltier, Tom Peltier, Jeff Sauntry, Quinn Shamblin, Brad Smith, and William Tompkins.

For more than a decade, SecureWorld has expanded and improved the concept of affordable regional security conferences. By ensuring knowledgeable speakers and quality educational and training programs, the security professional is able to stay current and cultivate contacts to help provide a means to get questions answered and problems solved. Mike O'Gara, Kerry Nelson, and the entire SecureWorld team are serving the industry well.

No one has all the answers to any question, so the really "smart" person cultivates good friends. Being in the information security business for nearly 40 years, I have had the great good fortune of having a number of such friends and fellow professionals. This group of longtime sources of great information includes John and Jane O'Leary, Lisa Bryson, Mike Corby, Terri Curran, Peter Stephenson, Merrill Lynch, Bob Cartwright, Pat Howard, Cheryl Jackson, Becky Herold, Ray Kaplan, Anne Terwilliger, David Lynas, John Sherwood, Herve Schmidt, Antonio and Pietro Ruvolo, Wayne Sumida, Dean Feldpausch, and William H. Murray.

My working buddies also need to be acknowledged. My son Justin was the greatest asset any father and information security team could ever hope for. Over the years, we logged thousands of air miles together and touched five continents. Every day I learned something new from him. I miss him greatly each and every day.

The other working buddy is John Blackley, a strange Scotsman who makes my life more fun and interesting. I've worked with John since 1985 and have marveled at how well he takes obtuse concepts and condenses them so that even management types can understand.

Who can leave out their publisher? Certainly not me. Rich O'Hanley has taken the time to discuss security issues with numerous organizations to understand what their needs are and then presented these findings to us. A great deal of our work here is a direct result of what Rich discovered that the industry wanted. Rich is not only the world's best editor and taskmaster but also a good friend and source of knowledge. Thanks, Rich!

Introduction

The purpose of information security is to protect an organization's valuable resources, such as information, computer hardware, and software. Through the selection and application of appropriate safeguards, security helps an organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. To many, security is sometimes viewed as thwarting the business objectives of an organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. Well-chosen security rules and procedures do not exist for their own sake—they are put in place to protect important assets and thereby support the overall business objectives.

Developing an information security program that adheres to the principle of security as a business enabler is the first step in an enterprise's effort to build an effective security program. Organizations must continually (1) explore and assess information security risks to business operations; (2) determine what policies, standards, and controls are worth implementing to reduce these risks; (3) promote awareness and understanding among the staff; and (4) assess compliance and control effectiveness. As with other types of internal controls, this is a cycle of activity, not an exercise with a defined beginning and end.

This book has been designed to give the information security professional a solid understanding of the fundamentals of security and the entire range of issues the practitioner must address. We hope that you will be able to take the key elements that comprise a successful information security program and implement the concepts into your own successful program. Each chapter has been written by a different author and will ensure that the reader gets the benefit of different ideas and approaches.

Information Security Fundamentals

Overview

The purpose of information security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps an organization to meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. We will examine the elements of computer security, employee's roles and responsibilities, and common threats. We will also examine the need for management controls, policies and procedures, and risk management. Finally, we will include current examples of procedures, policies, and examples that can be used to help implement the security program at your organization.

Elements of Information Security

Information security should be based on eight major elements:

1. Information security should support the business objectives or mission of the enterprise. This idea cannot be stressed enough. All too often, information security personnel lose track of their goals and responsibilities. The position of information security professional has been created to support the enterprise, not the other way around.
2. Information security is an integral element of fiduciary duty. Senior management is charged with two basic responsibilities: a *duty of loyalty*—this means that whatever decisions they make must be made in the best interest of the enterprise. They are also charged with a *duty of care*—this means that senior management is required to implement reasonable and prudent controls to protect the assets of the enterprise and make informed business decisions.

An effective information security program will assist senior management in meeting these duties.

3. Information security must be cost-effective. Implementing controls based on edicts is counter to the business climate. Before any control can be proposed, it will be necessary to confirm that a significant risk exists. Implementing a timely risk management process can complete this task. By identifying risks and then proposing appropriate controls, the mission and business objectives of the enterprise will be better met.
4. Information security responsibilities and accountabilities should be made explicit. For any program to be effective, it will be necessary to publish an information security policy statement and a group mission statement. The policy should identify the roles and responsibilities of all employees. To ensure third parties comply with our policies and procedures, the contract language indicating these requirements must be incorporated into the purchase agreements for all contract personnel and consultants.
5. System owners have information security responsibilities outside their own organization. Access to information will often extend beyond the business unit or even the enterprise. It is the responsibility of the information owner (normally the senior level manager in the business that created the information or is the primary user of the information). One of the main responsibilities is to monitor usage to ensure that it complies with the level of authorization granted to the user.
6. Information security requires a comprehensive and integrated approach. To be as effective as possible, it will be necessary for information security issues to be part of the system development life cycle. During the initial or analysis phase, information security should receive as its deliverables a risk assessment, a business impact analysis, and an information classification document. Additionally, because information is resident in all departments throughout the enterprise, each business unit should establish an individual responsible for implementing an information security program to meet the specific business needs of the department.
7. Information security should be periodically reassessed. As with anything, time changes the needs and objectives. A good information security program will examine itself on a regular basis and make changes wherever and whenever necessary. This is a dynamic and changing process and therefore must be reassessed at least every 18 months.
8. Information security is constrained by the culture of the organization. The information security professional must understand that the basic information security program will be implemented throughout the enterprise. However, each business unit must be given the latitude to make modifications to meet their specific needs. If your organization is multinational, it will be necessary to make adjustments for each of the various countries. These adjustments will

have to be examined throughout the United States too. What might work in Des Moines, Iowa, may not fly in Berkley, California. Provide for the ability to find and implement alternatives.

Information security is a means to an end and not the end in itself. In business, having an effective information security program is usually secondary to the need to make a profit. In the public sector, information security is secondary to the agency's services provided to its constancy. We, as security professionals, must not lose sight of these goals and objectives.

Information systems and the information processed on them are often considered to be critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources such as financial resources, physical assets, and employees. The cost and benefits of information security should be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed the expected benefits. Information security controls should be appropriate and proportionate.

The responsibilities and accountabilities of the information owners, providers, and users of computer services and other parties concerned with the protection of information and computer assets should be explicit. If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of control measures so that other users can be confident that the system is adequately secure. As we expand the user base to include suppliers, vendors, clients, customers, shareholders, and the like, it is incumbent upon the enterprise to have clear and identifiable controls. For many organizations, the initial sign-on screen is the first indication that there are controls in place. The message screen should include three basic elements:

1. The system is for authorized users only
2. Activities are monitored
3. By completing the sign-on process, the user agrees to the monitoring

More than Just Computer Security

Providing effective information security requires a comprehensive approach that considers a variety of areas both within and outside of the information technology area. An information security program is more than establishing controls for the computer-held data. In 1965, the idea of the "paperless office" was first introduced. The advent of third-generation computers brought about this concept. However, today, a vast quantity of all the information available to employees and others is still found in nonelectronic form. To be an effective program, information security must move beyond the narrow scope of IT and address the issues of enterprise-wide information security. A comprehensive program must touch every stage of the information asset life cycle from creation to eventual destruction.

Employee Mindset Toward Controls

Access to information and the environments that process them are dynamic. Technology and users, data and information in the systems, and the risks associated with the system and security requirements are ever changing. The ability of information security to support business objectives or the mission of the enterprise may be limited by various factors, such as the current mindset toward controls.

A highly effective method of measuring the current attitude toward information security is to conduct a "walkabout." After hours or on a weekend, conduct a review of the workstations throughout a specific area (usually a department or a floor) and look for just five basic control activities:

1. Offices secured
2. Desks and cabinets secured
3. Workstations secured
4. Information secured
5. Electronic media secured

When conducting an initial walkabout, the typical office environment will have a 90% to 95% noncompliance rate with at least one of these basic control mechanisms. The result of this review should be used to form the basis for an initial risk assessment to determine the security requirements for the workstation area. When conducting such a review, employee privacy issues must be remembered.

Roles and Responsibilities

As discussed previously, senior management has the ultimate responsibility for the protection of the organization's information assets. One of the responsibilities is the establishment of the function of Corporate Information Security Officer (CISO). The CISO directs the organization's day-to-day management of information assets. The Security Administrator should report directly to the CIO and is responsible for the day-to-day administration of the information security program.

Supporting roles are performed by the service providers and include Systems Operations, whose personnel design and operate the computer systems. They are responsible for implementing technical security on the systems. Telecommunications is responsible for providing communication services, including voice, data, video, and wireless.

The information security professional must also establish strong working relationships with the Audit staff. If the only time you see the audit staff is when they are in for a formal audit, then you probably don't have a good working relationship. It is vitally important that this liaison is established and that you meet to discuss common problems at least each quarter.

Other support groups include the Physical Security staff and the Contingency Planning group. These groups are responsible for establishing and implementing controls and can form a peer group to review and discuss controls. The group responsible for application development methodology will assist in the implementation of information security requirements in the application system development life cycle. Quality assurance can assist in ensuring that information security requirements are included in all development projects before moving on to production.

The Procurement Group can work to get the language of the information security policies included in the purchase agreements for contract personnel. Education and Training can assist in the development and conducting of information security awareness programs and for training supervisors in the responsibility to monitor employee activities. Human Resources will be the organization responsible for taking appropriate action for any violations of the organization's information security policy.

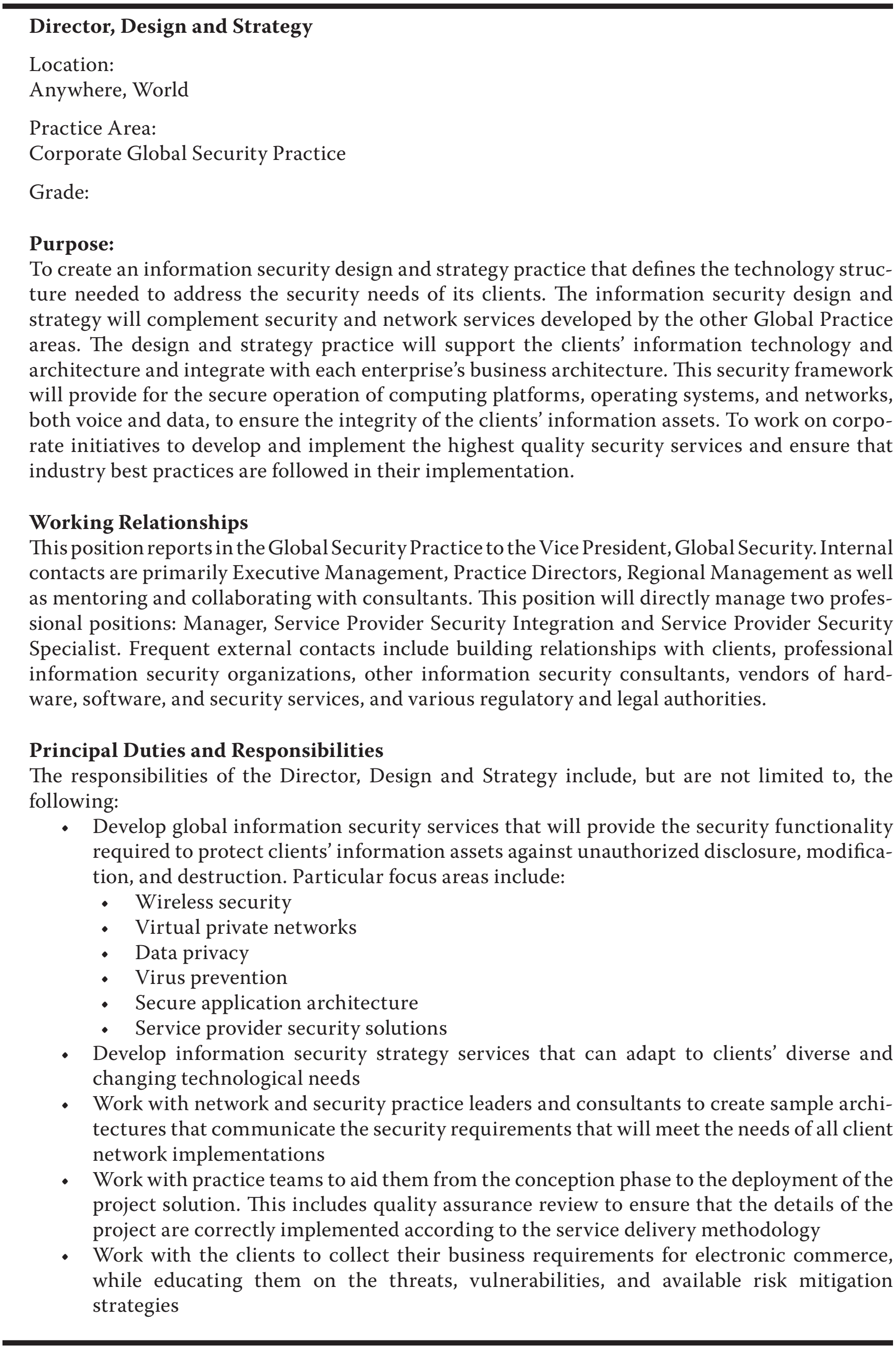
An example of a typical job description for an information security professional is shown in Figure I.1.

Common Threats

Information processing systems are vulnerable to many threats that can inflict various types of damage, resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire complexes. Losses can stem from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry. Precision in estimating information security–related losses is not possible because many losses are never discovered, whereas others are hidden to avoid unfavorable publicity.

The typical computer criminal is an authorized, nontechnical user of the system who has been around long enough to determine what actions would cause a "red flag" or an audit. The typical computer criminal is an employee. According to a recent survey in *Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare* by Richard Power, more than 80% of the respondents identified employees as a threat or potential threat to information security. Also included in this survey were the competition, contract personnel, public interest groups, suppliers, and foreign governments.

The chief threat to information security is still errors and omissions. This concern continues to make up 65% of all information loss problems. Users, data entry



Director, Design and Strategy

Location:
Anywhere, World

Practice Area:
Corporate Global Security Practice

Grade:

Purpose:
To create an information security design and strategy practice that defines the technology structure needed to address the security needs of its clients. The information security design and strategy will complement security and network services developed by the other Global Practice areas. The design and strategy practice will support the clients' information technology and architecture and integrate with each enterprise's business architecture. This security framework will provide for the secure operation of computing platforms, operating systems, and networks, both voice and data, to ensure the integrity of the clients' information assets. To work on corporate initiatives to develop and implement the highest quality security services and ensure that industry best practices are followed in their implementation.

Working Relationships
This position reports in the Global Security Practice to the Vice President, Global Security. Internal contacts are primarily Executive Management, Practice Directors, Regional Management as well as mentoring and collaborating with consultants. This position will directly manage two professional positions: Manager, Service Provider Security Integration and Service Provider Security Specialist. Frequent external contacts include building relationships with clients, professional information security organizations, other information security consultants, vendors of hardware, software, and security services, and various regulatory and legal authorities.

Principal Duties and Responsibilities
The responsibilities of the Director, Design and Strategy include, but are not limited to, the following:

- Develop global information security services that will provide the security functionality required to protect clients' information assets against unauthorized disclosure, modification, and destruction. Particular focus areas include:
  - Wireless security
  - Virtual private networks
  - Data privacy
  - Virus prevention
  - Secure application architecture
  - Service provider security solutions
- Develop information security strategy services that can adapt to clients' diverse and changing technological needs
- Work with network and security practice leaders and consultants to create sample architectures that communicate the security requirements that will meet the needs of all client network implementations
- Work with practice teams to aid them from the conception phase to the deployment of the project solution. This includes quality assurance review to ensure that the details of the project are correctly implemented according to the service delivery methodology
- Work with the clients to collect their business requirements for electronic commerce, while educating them on the threats, vulnerabilities, and available risk mitigation strategies

Figure I.1 Sample information security job description.

- Determine where and how cryptography should be used to provide public key infrastructure and secure messaging services for clients
- Participate in security industry standards bodies to ensure strategic information security needs will be addressed
- Conduct security focus groups with the clients to cultivate an effective exchange of business plans, product development, and marketing direction to aid in creating new and innovative service offerings to meet client needs
- Continually evaluate vendors' product strategies and future product statements and advise, which will be most appropriate to pursue for alliances, especially in the areas of:
  - Remote access
  - Data privacy
  - Virus prevention
  - Secure application architecture
  - Service provider security solutions
- Provide direction and oversight of hardware-based and software-based cryptography service development efforts

Accountability

Maintain the quality and integrity of the services offered by the Global Security Practice. Review and report impartially on the potential viability and profitability of new security services. Assess the operational efficiency, compliance to industry standards, and effectiveness of the client network designs and strategies that are implemented through the company's professional service offerings. Exercise professional judgment in making recommendations that may affect business operations.

Knowledge and Skills

- 40% Managerial/practice management
- Ability to supervise a multidisciplinary team and a small staff; must handle multiple tasks simultaneously; ability to team with other Practice Directors and Managers to develop strategic service offerings
- Willingness to manage or to personally execute necessary tasks, as resources are required
- Excellent oral, written, and presentation skills
- 10% Technical
- In-depth technical knowledge of information processing platforms, operating systems, and networks in a global distributed environment
- Ability to identify and apply security techniques to develop services to reduce clients' risk in such an environment
- Technical experience in industrial security, information systems architecture, design, and development, physical and data security, telecommunication networks, auditing techniques, and risk management principles
- Excellent visionary skills that focus on scalability, cost-effectiveness, and ease of implementation
- 25% Business
- Knowledge of business information flow in a multinational, multiplatform networked environment
- Solid understanding of corporate dynamics and general business processes; understanding of multiple industries
- Good planning and goal-setting skills
- 25% Interpersonal
- Must possess strong consulting and communication skills
- Ability to work with all levels of management to resolve issues
- Must understand and differentiate between tactical and strategic concepts
- Must be able to weigh business needs with security requirements
- Must be self-motivated

Figure I.1 (Continued) Sample information security job description.

Attributes

Must be mature, self-confident, and performance-oriented. Will clearly demonstrate an ability to lead technological decisions. Will establish credibility with personal dedication, attention to detail, and a hands-on approach. Will have a sense of urgency in establishing security designs and strategies to address new technologies to be deployed addressing clients' business needs. Will also be capable of developing strong relationships with all levels of management. Other important characteristics will be the ability to function independently, holding to the highest levels of personal and professional integrity. Will be an excellent communicator and team player.

Specific requirements include:

- Bachelor's degree (Master's degree desirable)
- Advanced degree preferred
- Fifteen or more years of information technology consulting or managerial experience, eight of those years spent in information security positions
- CISM or CISSP certification preferred (other appropriate industry or technology certifications desirable)

Potential Career Path Opportunities

Opportunities for progression to a VP position within the company

Figure I.1 (Continued) Sample information security job description.

personnel, system operators, programmers, and the like frequently make errors that contribute directly or indirectly to this problem.

Dishonest employees make up another 13% of information security problems. Fraud and theft can be committed by insiders and outsiders, but it is more likely to be done by employees. In a related area, disgruntled employees make up another 10% of the problem. Employees are most familiar with the organization's information assets and processing systems, including knowing what actions might cause the most damage, mischief, or sabotage.

Common examples of information security–related employee sabotage include destroying hardware or facilities, planting malicious code (viruses, worms, Trojan horses, etc.) to destroy data or programs, entering data incorrectly, deleting data, altering data, and holding data "hostage."

The loss of the physical facility or the supporting infrastructure (power failures, telecommunications disruptions, water outage and leaks, sewer problems, lack of transportation, fire, flood, civil unrest, strikes, etc.) could lead to serious problems and make up 8% of all information security–related problems.

The final area is malicious hackers or *crackers*. These terms refer to those who break into computers without authorization or exceed the level of authorization granted to them. Although these problems get the largest amount of press coverage and movies, they only account for 5% to 8% of the total picture. They are real, however, and they can cause a great deal of damage. But when attempting to allocate limited information security resources, it may be better to concentrate efforts in other areas. To be certain, conduct a risk assessment to identify what your exposure might be.

Policies and Procedures

An information security policy is the documentation of enterprise-wide decisions on handling and protecting information. In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organization strategy related to protecting both technical and information resources as well as guiding employee behavior.

When creating an information security policy, it is best to understand that information is an asset of the enterprise and is the property of the organization. As such, information reaches beyond the boundaries of IT and is present in all areas of the enterprise. To be effective, an information security policy must be part of the organization's asset management program and must be enterprise-wide.

There are as many formats, styles, and types of policy as there are organizations, businesses, agencies, and universities. In addition to the various forms, each organization has a specific culture or mental model on what and how a policy is to look and who should approve the document. The key point here is that every organization needs an information security policy. According to a recent industry report on computer crime, 65% of respondents admitted that they did not have a written policy. The beginning of an information security program is the implementation of a policy. The program policy establishes the organization's attitude toward information and announces internally and externally that information is an asset and the property of the organization and is to be protected from unauthorized access, modification, disclosure, and destruction.

This book will identify the key structural elements of policies and then review some typical policy contents. To assist you in the policy development process, an example of a recently implemented information security policy is included in Chapter 1, "Developing Policies."

Risk Management

Risk is the possibility of something adverse happening. The process of risk management is to identify risks, assess the likelihood of their occurring, and then take steps to reduce all risks to an acceptable level. All risk assessment processes use the same methodology. Determine the asset to be reviewed. Identify the threats, issues, or vulnerabilities. Assess the probability of the threat occurring, and the effect on the asset or the organization should the threat be realized (this is how a risk is determined). Then, identify controls that would bring the effect to an acceptable level.

The 2010 CRC Press book titled *Information Security Risk Analysis: Third Edition* discusses effective risk assessment methodologies. The book takes the reader through the theory of risk assessment:

1. Identify the asset
2. Identify the threats
3. Establish risk levels
4. Identify controls and safeguards

The book will help the reader understand qualitative risk analysis and then give examples of this process. To make certain that the reader gets a well-rounded exposure to risk analysis, the book presents eight different methods, finishing with the Facilitated Risk Analysis and Assessment Process (FRAAP). We will examine the FRAAP, and at the end of Chapter 4, a copy of a recent procedure on performing the FRAAP is included.

The primary function of information security risk management is the identification of appropriate controls. In every assessment of risk, there will be many areas for which the kind of controls that are appropriate will not be obvious. The goal of controls is not to have 100% security. Total security would mean zero productivity. Controls must never lose sight of the business objectives or mission of the enterprise. Whenever there is a contest for supremacy, controls lose and productivity wins. This is not a contest, though. The goal of information security is to provide a safe and secure environment for management to meet its fiduciary duty.

When selecting controls, it is important to consider many factors, including the organization's information security policy. Legislation and regulations that govern your enterprise, along with safety, reliability, and quality requirements, must also be factored into the process. Remember that every control will affect performance requirements in some way. These performance requirements may be a reduction in user response time, additional requirements before applications are moved into production, or additional costs.

When considering controls, the initial implementation cost is only the tip of the cost iceberg. The long-term costs for maintenance and monitoring must be identified. Be sure to examine any and all technical requirements and cultural constraints. If your organization is multinational, control measures that work and are accepted in your home country might not be accepted in other countries.

Accept residual risk. At some point, management will need to decide if the operation of a specific process or system is acceptable, given the risk. There can be any number of reasons that a risk must be accepted. These include but are not limited to:

- The type of risk may be different from previous risks
- The risk may be technical and difficult for a layperson to grasp
- The current environment may make it difficult to identify the risk

Information security professionals sometimes forget that the managers hired by our organizations have the responsibility to make decisions. The job of the security professional is to help the information asset owners identify risks to the assets, assist them in identifying possible controls, and then allow them to determine their action plan. Sometimes, they will choose to accept the risk and this is perfectly permissible.

Typical Information Security Program

Over the years, the computer security group responsible for access control and disaster recovery planning has evolved into the enterprise-wide information security group. Included in their ever-expanding roles and responsibilities are:

- Firewall control
- Risk management
- Business impact analysis
- Virus control and virus response team
- Computer emergency response team
- Computer crime investigation
- Records management
- Encryption
- E-mail, voice mail, Internet, video mail policy
- Social media usage policy and controls
- Enterprise-wide information security program
- Industrial espionage controls
- Contract personnel nondisclosure agreements
- Legal issues
- Internet monitoring
- Disaster planning
- Business continuity planning
- Digital signature
- Secure single sign-on
- Information classification
- Local area networks
- Remote access
- Security awareness programs

In addition to these elements, the security professional now has to ensure that standards, both in the United States and worldwide, are examined and acted upon where appropriate.

Summary

The role of the information security professional has changed over the past 25 years and will change again and again. Implementing controls to be in compliance with audit requirements is not the way in which a program such as this can be run. There are limited resources available for controls. To be effective, the information owners and users must accept the controls. To meet this end, it will be necessary for the information security professional to establish partnerships with its constituency. Work with your owners and users to find an appropriate level of controls. Understand the needs of the business or the mission of your organization. Make certain that information security supports those goals and objectives.

Editor

Thomas R. Peltier, CISSP (former CISM), has been an information security professional for over 35 years. During this time, he has shared his experiences with fellow professionals and, because of his work, has received the 1993 Computer Security Institute's (CSI) Lifetime Achievement Award. In 1999, the Information Systems Security Association (ISSA) bestowed on him its Individual Contribution to the Profession Award, and in 2001, he was inducted into the ISSA Hall of Fame. He was also awarded the CSI Lifetime Emeritus Membership Award. In 2010, Norwich University honored him with the 2010 Distinguished Faculty Award. He has retired from business and teaching.

Contributors

John A. Blackley, CISSP, a native of Scotland, has a total of 29 years' experience in information security—13 in large financial services companies and much of the balance leading practices in security consulting and healthcare. John has spent recent years focusing on information governance and risk management.

Maria Dailey is a graduate of Norwich University School of Business with a major in computer security and information assurance and a minor in computer crime and forensics. Maria has completed several courses focusing on information assurance, information security, number theory, and cryptology. Maria was involved in the EUCOM Combined Endeavor 2011 project during her junior year, working with classmates to develop and present a survey system to world leaders from more than 40 NATO and Partnership for Peace countries. Maria managed a small team of documenters and acted as lead technical writer. Maria is currently pursuing a career in digital forensics.

Patrick D. Howard, CISSP, CISM, is a senior cyber security consultant for SecureInfo, a Kratos Company. He has more than 40 years of experience in security, including 20 years of service as a U.S. Army Military Police officer, and has specialized in information security since 1989. Howard currently serves as the chief information security officer for the National Science Foundation's Antarctic Support Contract in Centennial, Colorado. He previously served as CISO for the Nuclear Regulatory Commission in Rockville, Maryland, from 2008 to 2012, and for the Department of Housing and Urban Development from 2005 to 2008. Howard was named a Fed 100 winner in 2007, and he is the author of three information security books: *The Total CISSP Exam Prep Book,* 2002; *Building and Implementing a Security Certification and Accreditation Program*, 2006; and *Beyond Compliance: FISMA Principles and Best Practices,* 2011. He is a member of the International Information Systems Security Certification Consortium's Government Advisory Board and Executive Writer's Bureau, which he chairs. Howard is also an adjunct professor of information assurance at Walsh College in Troy, Michigan. He earned a bachelor's degree from the University of Oklahoma in 1971 and a master's degree from Boston University in 1984.

Charles Johnson, CISSP, is an enterprise security and project management practitioner with more than 25 years of business information technology (IT) and consulting experience across banking, health care, hospitality, manufacturing, retail, and US/international government spaces. He is a multifaceted professional who applies his experience in information security, risk management, compliance, and physical security with project management to achieve more precise risk assessments, more accurate risk mitigation predictions, and regulatory compliance, which drives the implementation of effective, secure business solutions that add value and organizational efficiency.

Kimberly Logan, CISSP, CISM, is an information security officer working for the University of Cincinnati. She was graduated from Wright State University with a bachelor's degree in elementary education and worked as a substitute teacher in the Centerville, Ohio, school district before finding full-time employment with Electronic Data Systems (EDS). She began her career at EDS supporting the General Motors Acceptance Corporation (GMAC) branches and their System 38 and AS/400 midrange computers. When the GMAC branches began decommissioning the midrange computers, Kim was fortunate to be transferred to the security team. Kim worked as a mainframe security administrator for 5 years with EDS and was the team lead for 3 years. She moved to Cincinnati in 1999 and joined the UC security team. As a member of the information security team, Kim is responsible for risk management, security policy, and access control. She is a member of the International Systems Security Association (ISSA), the Information Systems Security Certification Consortium (ISC2), and the Information Systems Audit and Control Association (ISACA).

Kevin McLaughlin, CISM, CISSP, PMP, ITIL Manager Certified, GIAC Security Leadership Certificate, CRISC, began his career as a special agent for the U.S. government. He has had many careers over the years, including being a police officer in Kissimmee, Florida, an investigator for MasterCard/Visa, a middle school teacher, a director at the Kennedy Space Center (where he worked with Fred Hayes, James Lovell, Neil Armstrong, Alan Shepard, etc.), the president of his own company, an IT manager and senior information security manager with the Procter & Gamble (P&G) company, a CISO at the University of Cincinnati, and a senior information system security manager for the Whirlpool Corporation. Kevin has also been an adjunct college professor since 1992. While at P&G, Kevin created one of P&G's augmentation outsourcing teams in India. Kevin designed and implemented this India team, and it won a global Gold Service Award and has been a model for countless corporate relationships ever since. Over the years, Kevin has created an information security program, conducted information security strategic planning, designed information security solutions, investigated more than 700 cyber cases, and operated a global security operations center.

John G. O'Leary, CISSP, is president of O'Leary Management Education. A long-term IT practitioner, he has focused on computer security since the mid-1970s. John has designed, implemented, delivered, updated, and managed security awareness programs for organizations with populations ranging from tens to tens of thousands, computing platforms of varying ilk and vintage, networks spanning single sites to multiple nations, and very different information security needs. His background includes tours of duty in programming, systems analysis, auditing, project management, IT operations, production control, customer service, and quality assurance. He also taught every semester for 10 years at the University of Texas at Dallas Graduate School of Management, covering a wide range of management information systems courses. He has built and updated dozens of courses on virtually all aspects of information security, chaired, keynoted, planned and managed various computer security–related conferences for multiple organizations, and preached the value and methodologies of computer security to audiences around the world. He is the recipient of the 2004 COSAC Award, the 2006 EuroSec Prix de Fidelite, and the 2011 ISC2 Lifetime Achievement Award.

Justin Peltier, CISSP, CISM (February 29, 1976–October 17, 2011). He is missed.

Jeffery Sauntry, CISSP, CISM, CCFE, CFE, is a founding partner of Applied G2. He has more than 20 years of experience in enterprise-level information technology, security, governance, risk, and compliance, working with Fortune 500 companies and government clients. He leads billable engagements focused on optimizing efficiency, reducing operational and compliance risk by utilizing robust security capabilities that span technical, physical, and procedural compensating controls. Before joining Applied G2, Sauntry was the vice president of strategic programs for Unisys as part of an executive management turnaround team with the charter to create a unified strategy and go-to-market program for all security, compliance, and governance solutions for public sector and global industries market segments. Before his work at Unisys, he protected AT&T's Global 1000 Signature accounts security interest as the security practice director for AT&T Consulting. He has led engineering and professional services teams for numerous global security independent software vendors, including CA and Novell, as well as leading consulting firms KPMG and PWC.

Quinn R. Shamblin has served as an officer in the U.S. Navy, first as an instructor teaching nuclear power plant system theory, and then as the NPS director of multimedia development. Quinn moved from the navy to Procter & Gamble, where he worked as one of a team of three on the development, deployment, and support of a global data transport system. From there, he moved to Hydus Inc. as a business process automation architect. Quinn then joined the University of Cincinnati as a cybercrime investigator, information security manager, and then interim director of information security. He is currently the executive director of information security at Boston University. Quinn is also active in the information security community, having served as an officer in the Ohio chapter of the High Technology Crime Investigators Association for 2 years and as a contributor to a forensic blog run by SANS.

Brad Smith, RN, CISSP (March 18, 1953–December 6, 2012). His energy lives in us forever.

William Tompkins, CISSP, CBCP, is an information security officer at Teacher Retirement System of Texas. He has more than 28 years of experience in information technology and more than 20 years in information security, working for multiple government agencies for the state of Texas. Tompkins is an ISSA Distinguished Fellow and was elected to the Information Systems Security Association Hall of Fame in 2006. William holds two bachelor of science degrees, psychology and computer information Science, from Troy University in Alabama and a certification in risk management from the University of Texas at Austin, Division of Continuing Education.

Chapter 1

Developing Policies

Thomas R. Peltier

Contents

Policy Is the Cornerstone

The cornerstone of an effective information security architecture is a well-written policy statement. This is the source from which all other directives, standards, procedures, guidelines, and other supporting documents will spring. As with any foundation, it is important to establish a strong footing. As will be discussed, a policy performs two roles, one internal and one external.

The internal portion tells employees what is expected of them and how their actions will be judged. The external portion tells the world how the enterprise sees its responsibilities. Every organization must have policies in place that support sound business practices and they will demonstrate to the world that this organization understands that the protection of assets is vital to the successful execution of its mission.

In any discussion regarding written requirements, the term *policy* has more than one meaning. To some, a policy is senior management's directives on how a certain program is to be run, what its goals and objectives are, and to whom responsibilities are to be assigned. The term policy may refer to the specific security rules for a particular system such as Access Control Facility 2 (ACF2) rule sets, Resource Access Control Facility (RACF) permits, or intrusion detection system policies. Additionally, policy may refer to entirely different matters, such as specific management decisions setting an organization's e-mail privacy policy or Internet/social media usage policy.

Definitions

Policy

A policy is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area. When we hear discussions on intrusion detection systems monitoring compliance to company policies, these are not the policies we are discussing here. The intrusion detection system is actually monitoring standards (which we will discuss in more detail later), rule sets, or proxies. We will be creating policies like the policy on information security shown in Figure 1.1.

Later in this chapter, we will examine a number of information security policies and critique them based on an established policy template.

Standards

Standards are mandatory requirements that support individual policies. Standards can range from what software or hardware can be used, to what remote access protocol is to be implemented, to who is responsible for approving what. When developing an information security policy, it will be necessary to establish a set of supporting standards. Figure 1.2 is an example of what standards for a specific topic might look like.

Information Security Policy

Business information is an essential asset of the Company. This is true of all business information within the Company regardless of how it is created, distributed, or stored and whether it is typed, handwritten, printed, filmed, computer-generated, or spoken.

All employees are responsible for protecting corporate information from unauthorized access, modification, duplication, destruction, or disclosure, whether accidental or intentional. This responsibility is essential to Company business. When information is not well protected, the Company can be harmed in various ways such as significant loss to market share and a damaged reputation.

Details of each employee's responsibilities for protecting Company information are documented in the *Information Protection Policies and Standards Manual*. Management is responsible for ensuring that all employees understand and adhere to these policies and standards. Management is also responsible for noting variances from established security practices and for initiating corrective actions.

Internal auditors will perform periodic reviews to ensure ongoing compliance with the Company information protection policy. Violations of this policy will be addressed as prescribed in the *Human Resource Policy Guide for Management.*

Figure 1.1 Sample information security policy.

Information Systems Manager/Team Leader

Managers with responsibility for Information Systems must carry out all the appropriate responsibilities as a Manager for their area. In addition, they will act as *Custodian* of information used by those systems but owned by other managers. They must ensure that these owners are identified, appointed and made aware of their responsibilities.

All managers, supervisors, directors and other management level people also have an advisory and assisting role to IS and non-IS managers in respect of

- Identifying and assessing threats
- Identifying and implementing protective measures (including compliance with these practices)
- Maintaining a satisfactory level of security awareness
- Monitoring the proper operation of security measures within the unit
- Investigating weaknesses and occurrences
- Raising any new issues or circumstances of which they become aware through their specialist role, and
- Liaising with internal and external audit

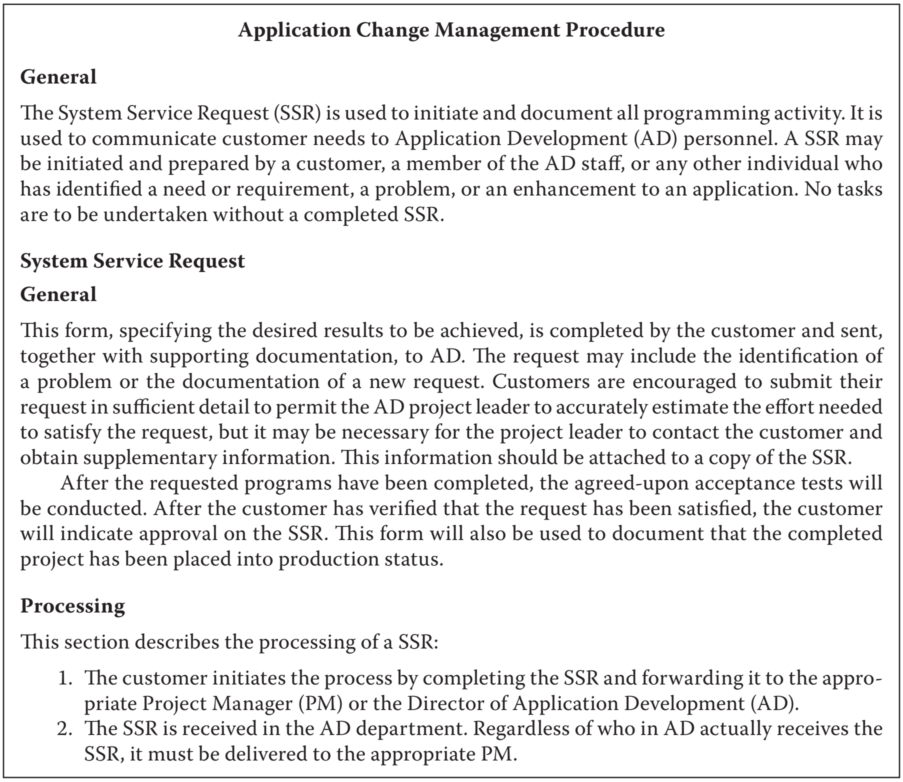
Figure 1.2 Example of standards.

Procedures

Procedures are mandatory, step-by-step, detailed actions required to successfully complete a task. Procedures can be very detailed. Recently, I was reviewing change management procedures and found one that consisted of 42 pages of precise information. It was very thorough and was what was needed to ensure that the process could be followed (Figure 1.3).

Guidelines

Guidelines are documented suggestions for the regular and consistent implementation of accepted practices. They usually have less enforcement powers. Where standards are mandatory, guidelines are recommendations. An everyday example of the difference between a standard and a guideline would be a "Stop" sign, which is a standard, and a "Please Keep off the Grass" sign, which would be nice, but it is not a law.



Application Change Management Procedure

General

The System Service Request (SSR) is used to initiate and document all programming activity. It is used to communicate customer needs to Application Development (AD) personnel. A SSR may be initiated and prepared by a customer, a member of the AD staff, or any other individual who has identified a need or requirement, a problem, or an enhancement to an application. No tasks are to be undertaken without a completed SSR.

System Service Request

General

This form, specifying the desired results to be achieved, is completed by the customer and sent, together with supporting documentation, to AD. The request may include the identification of a problem or the documentation of a new request. Customers are encouraged to submit their request in sufficient detail to permit the AD project leader to accurately estimate the effort needed to satisfy the request, but it may be necessary for the project leader to contact the customer and obtain supplementary information. This information should be attached to a copy of the SSR.

After the requested programs have been completed, the agreed-upon acceptance tests will be conducted. After the customer has verified that the request has been satisfied, the customer will indicate approval on the SSR. This form will also be used to document that the completed project has been placed into production status.

Processing

This section describes the processing of a SSR:

1. The customer initiates the process by completing the SSR and forwarding it to the appropriate Project Manager (PM) or the Director of Application Development (AD).
2. The SSR is received in the AD department. Regardless of who in AD actually receives the SSR, it must be delivered to the appropriate PM.

Figure 1.3 Sample of an application change management procedure.

3. If the PM finds the description of requirements on the SSR inadequate or unclear, the PM will directly contact the customer for clarification.

   When the PM fully understands the requirements, the PM will prepare an analysis and an estimate of the effort required to satisfy the request. In some cases, the PM may feel that it is either impossible or impractical to satisfy the request. In this case, the PM will discuss with the customer the reasons why the request should not be implemented. If the customer reaffirms the request, the PM and Director of AD will jointly determine whether to appeal the customer's decision to the Information Systems Steering Committee for a final ruling on the SSR.
4. If the project estimate is forty (40) hours or less, the detailed design should be reviewed with the customer. After design concurrence has been reviewed, the PM will project the tentative target date (TTD) for completion of the SSR. In setting the TTD, the PM will take into consideration the resources available and other project commitments. The TTD will be promptly communicated to the requesting customer.
5. If the project estimate exceeds forty (40) hours, the SSR and any supplemental project documentation will be forwarded to the ISSC for review, priority determination, and authorization to proceed.

   The committee will determine whether the requested change is to be scheduled for immediate implementation, scheduled for future implementation, or disapproved. If the request is disapproved, it is immediately returned to the customer, together with an explanation of the reason(s) for disapproval. If it is approved for implementation, a priority designation is made and the SSR is returned to AD for implementation scheduling.

   After implementation authorization has been received, the detailed design should be reviewed with the customer. After design concurrence has been received, the PM will project a TTD for completion of the project. In setting a TTD, the PM will take into consideration resources available and other project commitments. The TTD will be promptly communicated to the customer.
6. The PM will coordinate with AD personnel and other IT management and staff personnel (such as Database Administration, User Support Services, Network Administration, etc.) of their resources will be required to satisfy this request, or if there will be an operational or procedural effect in the other areas.
7. The PM will contact the customer to discuss, in detail, the test(s) that are to be conducted.
8. When Acceptance Testing (AT) has been completed, and the customer has verified the accuracy of the results obtained, the customer will indicate their approval to place the project into production by signing the SSR.
9. The Production Control Group (PCG) will place the project into production status. The PM will complete the bottom portion of the SSR, documenting that the project has been placed into production. The PM will log the status of the request as "completed" and file a copy of the SSR. The PM will promptly notify the customer that the project has been completed and placed into production.

Retention of Forms and Documentation

All documentation associated with the processing of each SSR will be retained for at least twelve (12) months.

Figure 1.3 (Continued) Sample of an application change management procedure.

Policy Key Elements

To meet the needs of an organization, a good policy should:

- *Be easy to understand*. It is important that the material presented meet the requirements of the intended audience. All too often, policies, standards, and procedures are written by subject experts and given to a general use audience. The material is often written at a college or technical level when the average reading and comprehension level in the workplace is that of a sixth grader (a 12-year-old).
- *Be applicable*. When creating policy, the writer may research other organizations and copy that document verbatim. This may be expedient; however, it is very important to ensure that whatever is written meets the needs of your specific organization.
- *Be doable*. Can the organization and its employees still meet business objectives if the policy is implemented? All too often, organizations implement policies to answer audit comments. The problem with doing this is that the policy may be so restrictive that it inhibits the ability to perform the business or mission of the organization.
- *Be enforceable*. Do not write a self-defeating policy. "Use of the Company-provided telephone is for business calls only." For most organizations, this may in fact be the policy, but almost every phone in the facility is used daily for personal calls. What might make a better policy is one that says, "Company-provided telephones are to be used for management-approved functions only." This opens up some latitude and still meets the business need.
- *Be phased in*. It may be necessary to allow the organization to read and digest the policy before it takes effect. Many organizations publish a policy and then require the business units to submit a compliance plan within a specific number of days after publication. This provides the business unit managers a period of time to review the policy, determine where their organization may be deficient, and then submit a timetable for compliance. These compliance letters are normally kept on file and are made available to the audit staff.
- *Be proactive*. State what has to be done, do not get into the rut of making pronouncements—"Thou shall not!" Try to state what can be done and what is expected of the employees.
- *Avoid absolutes*. Be diplomatic and understand the politically correct way to say things. When discussing sanctions for noncompliance, some organization have stated, "Employees violating this policy will be subject to disciplinary sanctions up to and including dismissal without warning." When the policy could have read something like, "Employees found in noncompliance with this policy will be deemed in violation of the Employee Standards of Conduct." The Standards of Conduct state that employees will suffer disciplinary sanctions up to and including dismissal. Where possible, use the kindlier, gentler approach.

- *Meet business objectives*. Security professionals must learn that controls must help the organization to an acceptable level of risk. One hundred percent security is 0% productivity. Whenever controls or policy affect the business objectives or mission or the organization, then the controls and policy will lose. Work to understand that the policy exists to support the business, not the other way around.

Policy Format

The actual physical format (layout) of the policy will depend on what policies look like in your own organization. To be successful, it is very important that any policy developed look like published policies from the organization. Find out who is responsible for policies at your organization and see if they have a template available. Some members of the review panel will be unable to read and critique the new policy if it does not look like a policy.

Policies are generally brief in comparison to procedures and normally consist of one page of text using both sides of the paper. In my classes, I stress the concept of brevity. However, it is important to balance brevity with clarity. Take all the words you need to complete the thought, but fight the urge to add more information.

Years ago, we had a young priest visit our parish and his homily that weekend included a discussion on the concept of imprinting. This concept is normally covered in a basic Psychology 101 class and is an early social behavior among birds and is a process that causes the newly hatched birds to become rapidly and strongly attached to social objects such as parents or parental surrogates. Although a number of parishioners understood what he was talking about, the majority of the parish just stared at him blankly. So he continued to add explanation after explanation until his homily lasted about 45 minutes. When writing a policy, balance the attention span time limit with what needs to be addressed. Keep it brief, but make it understandable.

There are three types of policies and you will use each type at different times in your information security program and throughout the organization to support the business process or mission. The three types of policies are

1. Global (tier 1)—these are used to create the organization's overall vision and direction
2. Topic-specific (tier 2)—these address particular subjects of concern. Where a typical tier 1 policy might address "Corporate Communications," the supporting tier 2 policies might address communication requirements when using e-mail, social media, voice mail, and other such methods
3. Application-specific (tier 3)—these focus on decisions taken by management to control particular applications (financial reporting, payroll, etc.) or systems (budgeting system)

Global Policy (Tier 1)

Under the Standard of Due Care, and charged with the ultimate responsibility for meeting business objectives or mission requirements, senior management must ensure that necessary resources are effectively applied to develop capabilities to meet the mission requirements. They must incorporate the results of the risk analysis process into the decision-making process. Senior management is also responsible for issuing global policies to establish the organization's direction in protecting information assets.

An information security policy will define the intent of management and its sponsoring body with regard to protecting the information assets of the organization. It will include the scope of the program, that is, where it will reach and what information is included in this policy. Finally, the policy will establish who is responsible for what.

The components of a Global Policy (Tier 1) typically include the following four characteristics.

Topic

The topic portion of the policy defines what specifically the policy is going to address. Because the attention span of readers is limited, the topic must appear quickly, in the opening or topic sentence. I normally suggest (note that it is a guideline, not a standard) that the topic sentence also include a "hook," that is, the reason I, as a reader, should continue to read this policy. So, in the opening sentence, we will want to convey two important elements: (1) the topic (it should have something to do with the title of the policy), and (2) the hook (why the reader should continue to read the policy).

An opening topic sentence might read as follows: "Information created while employed by the Company is the property of the Company and all employees must properly protect it."

Scope

The scope can be used to broaden or narrow either the topic or the audience or both. In an information security policy statement, we could say, "information is an asset and the property of the Company and all employees are responsible for protecting that asset." In this sentence, we have broadened the audience to include all employees. We can also say something like "Business information is an essential asset of the Company. This is true of all business information within the Company regardless of how it is created, distributed, or stored and whether it is typed, handwritten, printed, filmed, computer-generated, or spoken." Here, the writer broadened the topic to include all types of information assets.

Another example of broadening the scope might be as follows: "Information of the Company, its subsidiaries and affiliates in electronic form, whether being transmitted, or stored, is a key asset of the Company and must be protected according to its sensitivity, criticality, and value." Here, the topic subject is narrowed to "electronic form." However, the audience is broadened to include "subsidiaries and affiliates."

We can also use the scope concept to narrow the topic or audience. In an Employment Agreement policy, the audience is restricted to a specific group such as the following:

> The parties to this Agreement dated (specify) are (Name of Company), a (specify State and type of company) (the "Company") and (Name of Employee) (the "Executive").
>
> The Company wishes to employ the Executive, and the Executive wishes to accept employment with the Company, on the terms and subject to the conditions set forth in this Agreement. It is therefore agreed as follows:

Here, the policy is restricted to Executives and will then go on to discuss what can and cannot be done by the executives.

Responsibilities

Typically, this section of the policy will identify who is responsible for what. When writing, it is better to identify the "who" by job title and not by name. An Office Administrator's Reference Guide can be of great assistance by identifying how certain levels of management are referred to in communications. The policy will want to identify what is expected from each of the stakeholders.

Compliance or Consequences

When business units or employees are found to be in a noncompliant situation, the policy must spell out the consequences of these actions. For business units or department, if they are found in noncompliance, they are generally subject to an audit item and will have to prepare a formal compliance response.

For an employee, being found in noncompliance with a company policy will mean they are in violation of the organization's Employee Standards of Conduct and will be subject to consequences described in the Employee Discipline Policy.

Topic-Specific Policy (Tier 2)

Where the Global Policy (tier 1) is intended to address broad, organization-wide issues, the Topic-Specific Policy is developed to focus on areas of current relevance and concern to the organization. In support of the tier 1 "Corporate Communication Policy," management may find it appropriate to issue a policy on how an organization will approach social media usage or the use of the company-provided e-mail system. Topic-specific policies may also be appropriate when new issues arise, such as when implementing a recently enacted law requiring protection of particular information (GLBA, HIPAA, etc.). The Global Policy (tier 1) is usually broad enough that it does not require modification over time, whereas the Topic-Specific Policies (tier 2) are likely to require more frequent revisions as changes in technology and other factors dictate.

Topic-specific policies will be created most often by an organization. We will examine the key elements of the topic-specific policy. When creating an *Information Security Policies and Standards* document, each section in the document will normally begin with a topic-specific policy. The topic-specific policy will narrow the focus to one issue at a time. This will allow the writer to focus on one area and then develop a set of standards to support this particular subject.

Where the tier 1 policies are approved by the Information Security Steering Committee, the topic-specific (tier 2) policies may be issued by a single senior manager or director.

As with the tier 1 policies, tier 2 policies will address management's position on relevant issues. It is necessary to interview management to determine what their concerns are and what is it that they want to have occur. The writer will take this information and incorporate it into the following structure.

Thesis Statement

This is similar to the Topic section discussed in the tier 1 policies, but it also adds more information to support the goals and objectives of the policy and management's directives. This section will be used to discuss the issue in relevant terms and what conditions are included. If appropriate, it may be useful to specify the goal or justification for the policy. This can be useful is gaining compliance with the policy.

When developing a Workstation Standards document, a topic-specific policy on appropriate software, with supporting standards, might include a discussion on "Company-approved" software. This policy would define what is meant by company-approved software, which might be "any software approved, purchased, screened, managed, and owned by the organization." The policy would also discuss the conditions required to have software approved.

Once the terms and conditions have been discussed, the remainder of this section would be used to state management's position on the issue.

Relevance

The tier 2 policy also needs to establish to whom the policy applies. In addition to whom, the policy will want to clarify where, how, and when the policy is applicable.

Is the policy only enforced when employees are in the work-site campus or will it extend to off-site activities? It is necessary to identify as many of the conditions and terms as possible.

Responsibilities

The assignment of roles and responsibilities is also included in tier 2 policies. For example, the policy on company-approved software will have to identify the process to get software approved. This would include the authority (by job title) authorized to grant approval and a reference to where this process is documented.

This is a good time to discuss deviations from policy requirements. I have established a personal standard in that I never discuss how an entity can gain a dispensation from the policy. I don't like to state that "this is the policy and all employees must comply, except those of you that can find a way around the policy." Most organizations have a process to gain an approved deviation from a policy or standard. This normally requires the petitioner to submit a business case for the deviation along with alternative controls that would satisfy the spirit of the policy. If some organization or person wants a deviation from the policy, let them discover what the process is.

Compliance

For a tier 2 policy, it may be appropriate to describe, in some detail, the infractions that are unacceptable, and the consequences of such behavior. Penalties may be explicitly stated and should be consistent with the tier 1 Employee Discipline Policy. Remember, when an employee is found in a noncompliant situation, it is Management and Human Resources that are responsible for disciplining the individual.

Supplementary Information

For any tier 2 policy, the appropriate individuals in the organization to contact for additional information, guidance, and compliance should be indicated. Typically, the contact information would be specified by job title, not by individual name. It may also be prudent to identify who is the owner of this policy. This information will provide the reader with the appropriate information if they have suggestions on how to improve the policy.

To be effective, a policy requires visibility. Visibility aids implementation of the policy by helping ensure that it is fully communicated throughout the organization. Management presentations, videos, panel discussions, guest speakers, question and answer forums, and newsletters will increase visibility. The organization's Information Security Awareness Program can effectively notify users of new policies through the security blog or social media account. The New Employee

Orientation program can also be used to familiarize new employees with the organization's policies.

When introducing policies, it is important to ensure that management's support is clear, especially in areas where employees feel inundated with directives, regulations, or other requirements. Organization policies are the vehicles used to emphasize management's commitment to effective internal controls and their expectations for employee support and compliance.

Application-Specific Policy (Tier 3)

Global-level (tier 1) and topic-specific (tier 2) policies address policy on a broad level; they usually encompass the entire enterprise. The application-specific (tier 3) policy focuses on one specific system or application. As the construction of the organization information security architecture takes shape, the final element will be the translation of tier 1 and tier 2 policies down to the application and system level (tier 3).

Many security issue decisions apply only at the application or system level. Some examples of these issues include

- Who has the authority to read or modify data?
- Under what circumstances can data be read or modified?
- How is remote access to be controlled?

To develop a comprehensive set of tier 3 policies, use a process that determines security requirements from a business or mission objective. Try to avoid implementing requirements based on security issues and concerns. Remember, the security staff has been empowered to support the business process of the organization. Typically, the tier 3 policy is more free-form than tier 1 and tier 2 policies. As you prepare to create tier 3 policies, keep in mind the following concepts:

- Understand the overall business objectives or mission of the enterprise
- Understand the mission of the application or system
- Establish requirements that support both sets of objectives

Summary

In this chapter, we discussed that policy is the cornerstone of an organization's information security architecture. That a policy is important to establish both internally and externally what an organization's position on a particular topic might be. We defined what a policy, standards, procedure, and guideline is and what should be included in each of these documents or statements (Figure 1.4).

Sample Security Policy

I. Purpose

To provide direction regarding the protection of Michigan State Specific Agency (MSSA) *information resources* from unauthorized access, modification, duplication, destruction or disclosure.

II. Application

This policy applies to all MSSA personnel including employees, interns, vendors, contractors, and volunteers. This policy pertains to all information resources used to conduct MSSA business or used to transmit or store MSSA *Restricted* or *Confidential information*.

A MSSA information resource includes information that is electronically generated, printed, filmed, typed, stored or verbally communicated. Information resources must be protected according to its sensitivity, criticality and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed.

III. Definitions

1. *Information Resource*—any information created, stored in temporary or permanent form, filed, produced or reproduced, regardless of the form or media. Information includes, but is not limited to
   a. Personally identifiable information (PII)
   b. Reports, files, folders, memoranda
   c. Statements, examinations, transcripts
   d. Images, and
   e. Communications

   Information resources also include any electronically based system configured for the collection, processing, transmission, and dissemination of MSSA information resources. This includes, but is not limited to, software, hardware, and equipment such as servers, mainframes, midrange systems, telecommunications hardware, routers, switches, and software applications.
2. *Information Owner*—the Director of a MSSA Division where the information resource is created, or who is the primary user of the information resource.
3. *Business Owner*—where multiple information owners for the same information resource occur, the information owners must designate a Business Owner who will have authority to make decisions on behalf of all the owners of the information resource.
4. *Information Classification Categories*—all MSSA information shall be classified by the information owner into one of three classification categories:
   a. *Restricted*: This classification applies to information that is the most sensitive to MSSA and typically only a small number of personnel are authorized to view this type of information. The disclosure of this restricted information could have serious and damaging effects on MSSA and its partners. This type of information could include, but is not limited to, customer PII data (Social Security numbers, driver's license numbers, credit card numbers, etc.), human resource data (Social Security numbers, medical information, etc.), financial data, administrative passwords, encryption keys, litigation, archaeological site location information, and strategic planning documentation.
   b. *Confidential*: This classification refers to proprietary business information that is intended for use within MSSA for normal day-to-day responsibilities. Examples of this type of information could include, but are not limited to, policies, procedures, standards, business process flow diagrams, phone directories, organizational charts, archaeological collections, and documents labeled as confidential.

Figure 1.4 Sample security policy.

    c. *Public*: This classification applies to information that is approved for public access or to data whose disclosure would have no negative effects on MSSA. Examples could include, but are not limited to, agency announcements, publicly published phone numbers and addresses, general information about archaeological sites (excluding locations), and press releases.

5. *Reclassification*—the information owner is to establish a review cycle for all information classified as *Restricted* or *Confidential*, and reclassify it when it no longer meets the criteria established for such information. This cycle should be commensurate with the value of the information but should not exceed 1 year.
6. *Custodian*—the individual or entity designated by the information owner that is responsible for maintaining safeguards established by the information owner.
7. *Users*—authorized personnel who are responsible for using and safeguarding the information resources under their control according to the directions of the information owner.

IV. Policy

MSSA information resources residing in the various agency divisions are strategic and vital assets belonging to the people of Michigan. These assets shall be available and protected commensurate with the value of the assets. Measures shall be taken to protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Access to MSSA information resources shall be appropriately managed.

All MSSA personnel are accountable for their actions relating to information resources. Information resources shall be used only for intended purposes as defined by MSSA and consistent with applicable laws.

V. Responsibilities

1. The information owner has the responsibility to
    a. Identify the classification level of all information resources within their division
    b. Define and verify implementation of appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource
    c. Monitor the safeguards to ensure their compliance and report instances of noncompliance
    d. Authorize access to those who have a demonstrated business need for the information resource, and
    e. Remove access to those who no longer have a business need for the information resource
2. The *Custodian* has the responsibility to
    a. Implement integrity controls and access control requirements specified by the information owner
    b. Advise the information owner of any major deficiency or vulnerability encountered that results in a failure to meet requirements
    c. Comply with all MSSA-specific guidelines and procedures to implement, support, and maintain information security
3. The *Users* have the responsibility to
    a. Access only the information for which they have been authorized
    b. Use the information only for the purpose intended
    c. Ensure that authenticating information (e.g., password) is in compliance with existing MSSA/SOM security standards
    d. Maintain the integrity, confidentiality and availability of information accessed consistent with the information owner’s expectations while under their control

Figure 1.4 (Continued) Sample security policy.

e. Comply with all MSSA/SOM-specific guidelines and procedures to implement, support, and maintain MSSA/SOM Information Security policies and standards

f. Report violations or suspected violations of policies and standards to the appropriate MSSA management or the MSSA Information Security Project Manager

Access to information resources will be granted by the information owner to those with an approved business need. (Refer to MSSA Information Security *Access Control Policy.*)

VI. Compliance

1. The MSSA Division Directors (information owner) shall:
   a. Ensure there are adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity
   b. Manage MSSA/SOM information resources, personnel, and physical property relevant to MSSA's mission, as well as the right to monitor the actual utilization of all MSSA/SOM assets
   c. Ensure that all employees and contract personnel are aware of and accept their obligation to protect MSSA/SOM information resources
2. All authorized users (including but not limited to, agency personnel, temporary employees, and independent contractors) of MSSA information resources, shall formally acknowledge that they will comply with the information security policies and procedures of MSSA or they shall not be granted access to information resources.

Figure 1.4 (Continued) Sample security policy.

There are three types of policies and you will use each type at different times in your information security program and throughout the organization to support the business process or mission. The three types of policies are

1. Global (tier 1)—these are used to create the organization's overall vision and direction
2. Topic-specific (tier 2)—these address particular subjects of concern. We will discuss the information security architecture and each category such as the following
3. Application-specific policies—these focus on decisions taken by management to control particular applications (financial reporting, payroll, etc.) or systems (budgeting system)

Chapter 2

Organization of Information Security

Patrick D. Howard

Contents

The sixth clause of ISO 27002 focuses on the information security responsibilities of management within an organization. Specifically, it emphasizes the necessity of management commitment to the security of the organization's information resources. The importance of this topic is revealed in a cursory review of the 10 critical success factors identified in ISO 27002. Organizing for information security is

ISO 27002 CRITICAL SUCCESS FACTORS DIRECTLY RELATED TO ORGANIZING FOR INFORMATION SECURITY

- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture
- Visible support and commitment from all levels of management
- Process for funding of information security management activities
- Implementation and use of a system to measure information security management performance

SECONDARILY RELATED TO THE INFORMATION SECURITY ORGANIZATION

- Information security policy, objectives, and activities that reflect business objectives
- A good understanding of the information security requirements, risk assessment, and risk management
- Effective marketing of information security to all managers, employees, and other parties to achieve awareness
- Distribution of guidance on information security policy and standards to all managers, employees and other parties
- Providing appropriate awareness, training, and education
- Establishing an effective information security incident management process

directly related to four of these critical success factors, whereas the need of an organization to properly organize for its information security efforts indirectly relates to the remaining six as well. This chapter focuses on creation of a management framework to allow the organization to meet its information security objectives.

The Internal Information Security Organization

To protect their information assets, public and private organizations need to consider how best to manage their information security efforts. To ensure comprehensive protection for all the organization's information, the approach should address information security comprehensively, organization-wide. An enterprise-wide approach also facilitates management oversight and coordination of information security efforts. The design of the information security management framework should ensure it is properly tuned to the operational needs of the organization, which should primarily focus on the management of risks to its information assets. The satisfaction of organizational business needs will result in an information security function that is appropriately staffed, linked to the organization's strategic plan, integrated with organizational processes, and situated to optimize its visibility. It is impractical to stipulate minimum staffing level or organizational structure for the information security function. Consequently, each generic organization must assess its specific business needs related to the performance levels of tasks and implementation of processes normally associated with an information security function, which is described in the following paragraphs.

The design of the information security function must provide a management framework that permits effective initiation, implementation, and control of information security activities within the organization. This includes planning, coordination, and management of major information security projects, as well as monitoring, measuring, tracking, and overseeing the implementation of all aspects of the organization information security program. At a minimum, information security program management must include approval of information security requirements through their definition in an organization-wide information security policy, assignment of security roles and responsibilities, coordination of information security implementation throughout the organization, and an ongoing review of the adequacy and effectiveness of the program. The information security management function designed to meet these requirements must be appropriately positioned to serve as the arm of organizational management having the authority to develop and either approve or coordinate approval of an organization-wide information security policy, has the authority to define and assign or recommend assignment of information security roles, and is authorized to ensure coordination and implementation of organization-wide information security efforts.

The tasks the information security function is required to perform will also drive the design of the information security organization, and will normally include security program management, policy compliance monitoring and oversight, development and maintenance of security policy, security training and awareness, incident response and situational awareness, security architecture development and technical evaluation, and administration. The IT security organization should be designed to support the requirements of each of these functional areas, and distinct capabilities should be established for each.

Policy compliance and oversight activities should focus on management authorization activities, compliance reporting, information asset (system and facility) definition and inventory, security categorization/classification, plan of action and milestones (POA&M) and remediation tracking, interconnection agreement development and tracking, oversight of contractor operated systems, periodic independent review, and common controls definition. Necessary policy and training-related capabilities include development of policies, procedures, guidelines, and standards; managing exceptions and waivers; interpretation of policies; publication of policy notices; training and awareness for general users; provision of role-based and specialized security training; publication of periodic refresher messages; and dissemination of policy updates on current topics. Situational awareness and incident response capabilities should include containment, reporting, investigating, and coordinating the response to incidents, including the protection of evidence, as well as testing and evaluation of controls, system engineering, security architecture integration, consultation on system design, conducting threat analyses, vulnerability identification and tracking, trend analysis, assessment of new technology, interfacing with security operations, conducting penetration testing, vulnerability scanning, and performing forensic analysis.

To have the requisite level of authority, the information security function must be led by a member of the organization's management staff, and must be positioned in the organizational management structure where the visibility of information security can be ensured. Today, leadership of the information security organization resides at the executive level with most large organizations. The position of the Chief Information Security Officer (CISO) is widely recognized in both public and private sectors denoting the importance of information security in those agencies and companies. The appointment of a CISO or information security manager recognizes the need for dedicated leadership of an organization's information security efforts.

The process of organizing information security must address factors such as its mission, its composition, its placement within the organizational structure, its authority vis-à-vis other elements of the organization, its responsibilities, the functions it must perform, and its lines of communication and coordination. This process should begin with the identification of requirements for the information security function, which may include a review of the organization's mission, strategic plan, and legislation, contracts, and other external directives and regulations that may potentially drive information security efforts. Directions and observations from senior agency executives should also be considered as part of the requirements identification.

An inventory of all security-related activities and resources in the organization should be developed to understand who is currently performing information security roles and functions. A determination of where information security is performed in the organization and those who are performing information security tasks serves as a basis for the formulation of a coherent strategy and for the design of an effective information security function. Introduction of benchmarking and leading practices can then be used to define the organization's approach to information security management and permits the identification of the target information security function according to known requirements affecting information security. Based on knowledge of the current state of the organization's information security posture, as well as the future state, organizations must then perform a gap analysis to identify unmet requirements, and a path forward for meeting them.

The organization should clearly define the boundaries of the information security function to address interfaces with other internal elements that perform security-related functions. These may include, for example, information technology operations, personnel security function, privacy staff, and the physical security office. These relationships should be documented in coordinated operational agreements (i.e., charters, concepts of operations or CONOPs, procedures, etc.).

The CISO or information security program manager must have the authority to task other elements of the organization to perform certain security functions defined by the organization. For example, the manager must have the authority to direct business units to periodically update security documentation, or to perform security activities following defined processes. Their authority must include investigation of incidents and security violations when they occur. The information security management function should be able to enforce information security requirements, or at least be able to rely on the organizational managers to take corrective action when violations or incidents occur. With the latter arrangement, the CISO must establish strong working relationships with business unit management to ensure that proper disciplinary action is taken in response to violations to prevent their reoccurrence.

Visibility of the information security program is a major factor in determining where the information security function should be organizationally located. Organizational placement influences the ability of the CISO to gain access to upper management. To ensure the proper level of visibility, the information security function cannot be buried deep within the organizational structure, and the CISO should not have to struggle to obtain the attention of upper management.

In larger organizations, the need for independence of the information security function must be considered. Because of compliance responsibilities, the information security function should be fully independent of organizational elements subject to the security policy. This separation is essential for providing assurance that business units are not capable of hindering compliance monitoring activities. Consequently, the independence of the information security function should be evident throughout the organization. Information security function independence should also include control of its own budget and resources, as well as a separate operating space to permit proper protection of its own sensitive data.

To formalize the information security organization, consideration should be given to developing several key documents consistent with the organization's procedures and culture. A mission statement should be used to document what the office is chartered to accomplish. The CISO or information security manager should create a vision statement to define how they envision accomplishment of the mission. A documented value proposition helps set the expectations for those affected by the information security function, and provides a benchmark on which to evaluate the information security services performed. To establish how the office will function, standard operating procedures are required to provide members of the information security organization steps necessary to perform routine, recurring tasks. To guide external customers, a documented concept of operations is necessary to address activities such as penetration testing, weakness remediation, contingency planning and testing, and annual controls testing. An operating plan for the function defines the goals and objectives to be achieved over a relatively long period of time, normally 3 to 5 years. It provides milestones to be achieved and establishes priorities and sequences for tasks that the organization must perform. Development of the operating plan must be consistent with the overall agency strategic plan and IT strategic plan.

In the following paragraphs, critical components of an organization-wide information security function are described. This includes a discussion of the importance of management support for information security, mechanisms for coordination and communication of information security requirements, assignment of information security roles and responsibilities, management authorization of information systems, development and use of confidentiality agreements, the independent information security review process, and considerations for dealing with external parties having access to organization information.

Management Support

ISO 27002 emphasizes the importance of management support in paragraph 6.1.1, referring to it as "management commitment to information security." It establishes the need for active management support organizational information security efforts by providing clear direction, demonstrating its commitment to information security, explicitly assigning information security responsibilities, and by acknowledging its own responsibilities for information security. Support that meets this standard must be visible, effective, focused, outcome-oriented, and its existence should be obvious across the organization. Management must provide information security direction that is expressed in understandable terms and is consistent over time. Organization management can demonstrate its commitment by following up on its policy pronouncements with observable action. Management must show interest in information security and maintain appropriate involvement in program initiatives and activities. Management must show active support by willfully assigning information security responsibilities to organization personnel to establish accountability for the accomplishment of key duties and tasks. Management must also recognize its own responsibility for information security by communicating this fact both in written and oral means. Management support that does not meet this standard could result in less than necessary emphasis on the importance of information security to the organization and its mission, thereby diminishing its effectiveness.

The means by which management can ensure that it provides adequate support to information security can be promoted through management actions in the areas of planning, policy, visibility, resources, accountability, awareness, and efficiency. Specific management support considerations are as follows:

- It is within management's purview to ensure that the goals for the security of organization information are established through strategic and tactical planning, and are maintained, emphasized, and measured. These goals must serve to address organizational business requirements, must be both realistic and achievable, and must be regularly measured to ensure that they are in tune with enterprise risk management and mission requirements. Management should also ensure that security goals are considered in capital investment planning, project management, organizational staffing, acquisitions, performance measurement, and other organizational processes.
- Management must act to ensure the organization has a mechanism for creating an information security policy that facilitates goal achievement. Management must also ensure that the policy is properly coordinated across the organization, and is properly vetted and approved. These actions ensure that the policy satisfies organization level, enterprise-wide business requirements.
- Management must ensure the approved information security policy is properly implemented and consequently must take action to ensure that it has a mechanism for monitoring implementation activities for effectiveness. This is the policy oversight and compliance function facilitated by activities of the information security organization and management's own program oversight committee. Such oversight bodies are most effective when formally chartered, and when membership, authority, and goals are defined.
- Organizational management must render appropriate direction and support for initiatives relating to its information security program. This may be an awareness campaign, rollout of a new security strategy, or introduction of a new security process or solution. The information security function will define aspects of the security initiative in its plans and will present them to management for approval as a basis for management support. Once management concurs with the objectives and parameters for the initiative, it should be visibly involved in ensuring the initiative's success according to the plans developed to meet those objectives. Through such efforts, management can promote and foster a culture of security.
- On the basis of the approved plans, management should provide additional support to information security initiatives through the provision of necessary resources, for both funding and personnel. This may also include giving priority to information security by directing other organizational elements to support information security requirements initiatives. This may include actions related to the completion of information security training, adherence with processes, compliance with policy, and implementation of security controls. To facilitate management support of this nature, the information security function must adhere to organizational requirements for obtaining resources such as budget formulation, manpower planning, capital investments, etc.

- Organizational management must support information security efforts by defining in policy or through other formal means the roles and responsibilities for the entire agency, and also establishing information security requirements and qualifications for the assignment of personnel. This may involve publication of assignment orders, appointment memos, and integration of information security responsibilities in job descriptions and performance plans. These actions permit the establishment of accountability for information security.
- Ongoing awareness of information security must be emphasized by organization management to recognize the importance of personnel in the security of information. Management is responsible for ensuring the existence of plans and programs for making this happen. Plans may include the identification of audiences, topics, frequency, type, and duration of awareness training. Programs may include mechanisms for testing awareness and updating training content to ensure that it is realistic, responsive to existing threats, and meets current business needs. Management should recognize that awareness efforts can enhance security by increasing user engagement with the information security program.
- Management is also responsible for ensuring that security controls are implemented in a coordinated fashion organization-wide. Effective coordination can result from the actions of the information security function supported by the oversight/steering committee and other lower level, cross-organization coordination committees or working groups. The identification and implementation of common controls for the protection of multiple systems and information assets also fosters effective coordination by meeting the objectives of consistency, efficiency, cost-effectiveness, and interoperability of controls. Management can also foster effective information security coordination by stressing the importance of sound project management and integration of information security into the organization's system development life cycle methodology and practices.

Information Security Coordination and Communications

ISO 27002 emphasizes the importance of properly coordinating information security within the organization and maintaining effective contacts to effect communications with external authorities, specialists, and interest groups. Sections 6.1.2, 6.1.6, and 6.1.7 detail the requirements for program coordination and communication. The following paragraphs synthesize considerations for effectively coordinating and communicating information security program activities.

Information Security Coordination

The security of organization information requires a multidisciplinary approach involving virtually all organizational elements and personnel. Information security activities and requirements should therefore engage expertise available within the organization to include the general counsel, public affairs, facility security and engineering, personnel security, union management, human resources, training, contracting, finance, internal audit, information technology operations, system development, capital planning, insurance, enterprise architecture, privacy, and records management. Representatives of these activities who are assigned relevant roles and job functions should be involved in the coordination of information security activities and, where necessary, should be formally assigned security roles and responsibilities as detailed below. Representatives [e.g., information system security officers (ISSOs), system administrators, developers, auditors, project managers, and information technology operations personnel] should be provided specialized information security training to better prepare them to perform their responsibilities. In large organizations, information security coordination may be facilitated through an existing management group such as an information technology governance committee or through a specialized information security committee (e.g., ISSO forum). In smaller organizations, this coordination may be performed by another management group or an individual manager.

The objective of cross-organization coordination should be collaboration and cooperation. The objective is to effectively integrate information security into the operations of all elements of the organization, and the information security function must collaboratively work together with business units to obtain their input to inform decisions regarding the definition of requirements, priorities, strategies, and timetables. Coordination of this type should result in joint identification of and consensus in goals established for the information security program. Other considerations for information security program coordination include

- All information security–related activities should adhere to the information security policy. To ensure consistency of performance and compliance with established requirements, the information security function should be in a position to review all activities against the policy.
- Coordination activities should assure that the policy is enforced through the development of coordinated processes for identifying, communicating, and dealing with policy violations and situations involving noncompliance.
- All information security methodologies and processes such as risk assessment, information classification, vulnerability remediation, and system authorization should be coordinated across the organization to ensure that they meet organizational needs and requirements, are based on leading practices, and are consistent with the information security policy. To achieve this goal, the organization must ensure that there are mechanisms for their development, dissemination, review, validation, finalization, and maintenance.
- The organization must have the capability to identify significant changes in threats to its information and to coordinate a unified response to them with all affected organizational elements. This threat identification capability must

ensure that threats are assessed, prioritized, communicated, and countered with the degree of urgency warranted by the threat.

- Implementation of information security controls and assessment of their adequacy requires effective coordination focused on compliance with the policy, reliance on approved security mechanisms and procedures, and recognition of the inherent risks involved. The information security function must ensure that the efforts of system owners, ISSOs, engineers, developers, auditors, and program managers lead to effective implementation and maintenance of controls protecting the organization's information.
- Effective coordination ensures that information security education, training, and awareness activities are promulgated throughout the organization. This ensures consistency in the performance of organization personnel in information security and fosters an organizational culture of security.
- The capability to coordinate the results of information security–related monitoring and review activities leads to the effective implementation of appropriate actions in response to security incidents and identified vulnerabilities. A process such as this ensures that the organization is able to apply lessons learned enterprise-wide to effectively respond to situations and avoid their recurrence elsewhere.

Contact with Authorities

The organization should establish contacts with relevant authorities to keep up with industry trends, to monitor standards, to gain knowledge of security methodologies and processes, and to provide liaison points for handling information security incidents. These contacts may be formed on the basis of formal contractual arrangements, subscriptions, membership, or may be informal in nature consisting of personal contacts, calls, and meeting attendance. Contacts with authorities may include industry groups; incident response authorities (e.g., the U.S. Computer Emergency Readiness Team or US-CERT); consulting houses; higher headquarters; Federal, State, and local law enforcement officials; and relevant sister organizations.

Organizations whose responsibility is to make the contact must manage these contacts by developing procedures to specify when authorities should be contacted and the definition of the manner in which the identified information security incidents are to be reported, including timeframes for reporting by type of incident—particularly when laws are suspected of having been broken. Organizations must make provisions in advance by defining the process for obtaining assistance from external third parties (e.g., an Internet service provider or telecommunications operator) in the event of an attack so that they can take action against the source of attack. These processes not only support information security incident management but also business continuity and contingency planning process. Also, contacts with regulatory entities provide the organization useful information to allow anticipation and preparation for potential changes in legislation, regulations, and guidance that the organization must adhere to. These contacts may be with higher headquarters, legislative affairs organizations, industry groups, and government-wide forums. Additionally, the organization should maintain contacts with other types of authorities related to the security of its information, which may include utilities companies, emergency service organizations, fire departments, telecommunication providers, and emergency health and safety personnel.

Contact with Special Interest Groups

The information security organization should identify needs for both internal and external specialized information security advice and information. The organization should have a process for assuring the value and credibility of information received, and disseminating it to the appropriate recipients in a timely fashion. The information security function should be charged with maintaining ongoing contact with groups that provide information related to information security awareness, best practices, and lessons learned. This includes specialist security forums and professional associations. Examples include software vendors that provide vulnerability and patching information regarding their products. The International Information Systems Security Certification Consortium or (ISC)^2, SysAdmin, Audit, Networking, and Security (SANS) Institute, and other organization host sites wherein specialty information security advice and assistance can be located. Government and industry groups that share information security concerns are another source of specialty information, particularly with respect to compliance with legislation (e.g., Health Information Portability and Accountability Act; Federal Information Security Management Act). Also, informal contacts with counterparts outside the organization by the CISO or information security manager can be highly valuable in sharing experiences and best practices.

Contacts of this type gives the organization access to alerts, warnings, and patches relating to attacks on and vulnerabilities in the organization's technologies. These groups also provide information that permits an understanding of the broad information security environment including current threats, vulnerabilities, and attack trends. Specialty sources can be useful in obtaining and exchanging information regarding new security technologies, products, and processes, and in providing advice on best practices for information security and implementation of security controls. Finally, these groups provide avenues for reporting information about security incidents to foster cooperation and information sharing.

Information Security Roles and Responsibilities

All information security roles and responsibilities should be formally allocated by defining them in writing using terms that are clearly understood across the organization. This includes specification of responsibilities for the protection of individual assets as well as for performing specific security tasks. This will ensure that those assigned to information security–related positions are delegated the authority necessary to perform the work as well as the establishment of accountability for personnel assigned those tasks. Assignment of information security responsibilities also ensures consistency in the allocation of key program responsibilities throughout the entire organization. This action is one of the primary information security functions of organization management and should be performed according to the information security policy. Linkage of this activity to the policy requires review of roles and responsibilities whenever the policy is updated, and although roles and responsibilities do not necessarily have to be a documented part of the policy, they must adhere to it.

Documentation of information security responsibilities should be specific enough to define, at a high level, what the role entails. As necessary, more detailed guidance should be issued to supplement this high-level role description. Additionally, responsibilities and supplementing procedures should be tailored to the needs of specific locations, facilities, and operations as necessary. For instance, the responsibilities for the data center security manager should significantly differ from those of a network security manager. Similarly, local conditions should lead to the specification of detailed responsibilities for specific security processes such as vulnerability scanning and contingency planning. Each organizational element will ensure that information security responsibilities are appropriately modified or supplemented to meet its own local business needs.

An individual who is assigned information security responsibility may delegate security tasks to another, yet must remain responsible for ensuring that the tasks are performed correctly. For example, the owner of an information system may choose to delegate responsibility for performing system level security tasks to an ISSO. Or an authorizing official who has a multitude of other duties may delegate his or her security tasks to a designated representative for performance. In each case, the system owner and authorizing official maintain responsibility for ensuring that these delegated tasks are properly performed. This approach ensures that security tasks are performed in a responsible manner while maintaining accountability for their completion.

With respect to responsibility for areas, assets, and processes, individuals may need a clear definition for all assets and processes associated with a particular information system. This pertains to the hardware, software, procedures, user base, data, and controls within the boundaries of that system. The terms and limitations of management's authorization of an information system or facility should also be clearly defined. How the asset will be used and its purpose will be made known to the responsible individual to ensure their understanding of their responsibilities.

In large organizations, the CISO or information security manager will be assigned overall responsibility for the information security program. Nevertheless, individual managers typically maintain responsibility for resourcing and implementing program requirements. The appointment of an owner for each information asset facilitates the assignment of responsibility for the ongoing security of that asset. This approach recognizes the span of control of information security management while providing for effective security policy compliance and accountability for the performance of security tasks.

Management Authorization

Organizations should establish and implement a process for management to authorize the use of critical information assets. This typically pertains to information processing facilities, information systems, and applications. It may also include capabilities and processes considered to pose an increased risk to information (e.g., remote access and use of personally owned assets). This provides a means for management to exercise its responsibility for ensuring it has considered the risks associated with its most important assets and most risky operations. In most organizations, the CISO or information security manager defines, implements, and maintains oversight of the authorization process.

Management authorization is implemented in the U.S. Federal Government through the designation of authorizing officials who are senior management officials empowered to authorize the operation of government information systems. Each agency must identify who performs the authorizing officials' function and must prepare them to perform this role. The number of authorizing officials depends chiefly on the number of information systems an agency has and how the agency is organizationally structured. To be effective, authorizing officials must be familiar with the requirements of their role to include knowledge of the agency's business processes and understanding risk management principles. The CISO must ensure that each authorizing official is aware of the critical aspects of the position by documenting requirements, providing training upon their initial assignment to the role, and then keeping them apprised of changes in the threat environment.

Where information assets are interconnected or are otherwise interdependent, authorization should consider the effect such assets may have on the organization's level of risk. Authorization should take place before use to ensure that relevant security requirements are met and risks are identified and mitigated.

Confidentiality Agreements

According to ISO 27002, confidentiality and nondisclosure agreements are designed to protect an organization's information and inform those signing the agreement of their responsibility for the information's responsible and authorized protection, use, and disclosure. They provide management another control mechanism to exercise its information security responsibilities. Directed at the internal workforce, nondisclosure agreements specify the organization's requirements for protecting its information against unauthorized disclosure. This serves as an effective means for organizations having a need for protection of information confidentiality, but does not address requirements for maintaining its integrity or availability. Such agreements provide a basis for legal action in the event of unauthorized disclosure, which may include administrative penalties, termination, lawsuit, or criminal prosecution.

The contents of the confidentiality agreement should include the specification of its scope (i.e., classified, sensitive, restricted, related to a specific project, etc.); the terms of the agreement (for example, upon declassification of the information, 1 year following termination, etc.); specific actions to be taken upon its termination (e.g., notifications, information disposition, etc.); specific responsibilities of employees or other signatories to protect the confidentiality of information against unauthorized disclosure; specifying who "owns" the information and therefore who can make decisions about its protection requirements, disposition, handling, disposal, marking, downgrade, modification, alteration, etc.; specifying the limits over the use of the information; definition of the notification and reporting process for disclosure breaches, and procedures for notification in the case of violations of the agreement; and stipulation of the right to audit and monitor security involving confidential information. Once the agreement is signed, the receiving party agrees to allow its activities to be audited and monitored to provide assurance that confidentiality is protected.

The organization's general consul or legal department should review all nondisclosure agreements to ensure that they comply with all applicable laws and regulations. The organization should periodically review its requirements for confidentiality agreements and also when changes occur to influence requirements.

Information Security Program Review

Organization management has an obligation to ensure that efforts to protect its information are adequate. A process for reviewing the information security program is essential to ensuring that compliance with established information security requirements is maintained, gaining assurance that relevant risks are addressed, and maintaining awareness of the effectiveness of program controls. This process should focus on periodic review of the program by an independent entity as well as when significant changes affecting security occur. The scope of this review should include the implementation of security controls, processes, and procedures with respect to how they meet established information security policy requirements. To optimize scheduling and to establish clear authority, organization management is responsible for directing program reviews, and for addressing the resulting findings and recommendations.

The scope and methodology used in reviews should be tailored to organizational needs, which vary over time. Application of a variety of assessment approaches focused on various components of the information security program or information assets is advisable. For instance, penetration testing may be employed to determine the effectiveness of specific perimeter-protective mechanisms in preventing or detecting external attacks, or may include evaluation of all perimeter controls. This should be augmented by regular security controls testing of particular information systems, components, or facilities. Additionally, a periodic review of the entire information security program ensures that all aspects of the organization's information security efforts are comprehensively reviewed for adequacy. A broad-based program review of this type is normally performed by the internal audit function. Management must ensure that personnel conducting information security reviews are independent of the subject of the review and have the appropriate skills and experience necessary to perform the review, including expertise in the technologies to be reviewed, and in accepted assessment and audit methods. This is achieved through definition of skills and independence requirements and validation by the information security function. The results of the review should be formally documented to demonstrate the organization's due diligence, and reported to management for review upon conclusion of review activities.

Management's response to independent reviews should focus on determining the effectiveness and adequacy of the organization's approach to managing and implementing information security according to its stated security policy and current view of risks to the organization's information. Management should require corrective action to be taken to address all identified weaknesses, and must insist on a process for tracking the status of completion.

External Parties

Special provisions need to be taken to protect organizational data in cases where it must be accessed, processed, communicated to, or managed by external parties. This may be through formal relationships with customer organizations, arrangements with supporting vendors, communications with a superior organization, or any other external entity with which information is exchanged. ISO 27002 provides examples of external parties, including service providers (ISPs, network providers, telephone services, and maintenance and support services); managed security services; customers; providers of facilities or operations (IT systems, data collection services, and call center operations); business consultants and auditors; developers and suppliers of software products and IT systems; cleaning, catering, and other outsourced support services; and temporary personnel, students, and other short-term personnel. Arrangements along these lines generally do not include information exchanges with entities within the same management authority and organizational structure. The guiding principle for dealing with external parties of this type is to ensure that the security of the organization's information and information processing facilities is not to be diminished through the introduction of external party activities, products, or services. Should this occur, the agreement with the external party should be suspended or terminated immediately to prevent further risk to the organization's information. To prevent these risks, any access to the organization's information by external parties should be fully understood and controlled because surrender of control by the information owner means there is no assurance that security is maintained.

Before engaging in an arrangement for external data access (e.g., cloud solutions and services), management must determine that there is a bona fide business requirement for external parties to have access to the organization's information assets, or to begin use of a product and service provided by an external party. Management must ensure it is aware of the security impacts of such an arrangement before making such a decision, and a risk assessment should be conducted to establish the implications and requirements associated with the potential relationship. The risks associated with these arrangements need to be formally addressed by the use of an acceptable risk assessment methodology. The purpose of the risk assessment is to ensure that the organization understands the security impacts of the proposed connection/exchange, and to identify requirements for security controls. Alternatively, changes in the conditions for the use of an established information system or facility may be addressed in a security impact assessment of changes brought on by the external connection or information access.

On the basis of the risk assessment, requirements for the protection of the organization's information can then be documented in interconnectivity agreements, contract provisions, and security clauses of memoranda of understanding for organizations and agreements on rules of behavior for access by individuals such as customers, consultants, vendors, and staff of supporting organizations.

Assessment of External Risks

When identifying risks related to access by external parties, organizations should complete that activity and implement necessary controls before actually granting access to its information. This minimizes the risk of introducing a new threat without the organization first having assessed and countered it. The organization granting access to its information has the responsibility of determining the appropriateness of controls and whether or not to grant access without first having all necessary controls in place. Management's responsibility also includes continuing actions to ensure that the terms of the agreement are met, and that the security of its information is maintained.

The assessment should consider all facilities and assets to be affected when assessing the risks associated with access by external entities. All hardware, software, processes, and facilities must be included in the scope of the risk assessment. The nature of the information access that the external party will have (physical access, logical access, direct system connectivity, remote access, on-site and off-site access, etc.) should also be a focus of the assessment. The criticality and sensitivity of the information to be externally accessed according to its need for confidentiality, integrity, and availability should be a significant aspect of the risk assessment. The risk assessment effort must identify the controls needed to restrict external access to organization information not within the scope of the proposed agreement to ensure its protection through segregation. The effort must address the risks of personnel who will have access to the organization's information and the process for ensuring their trustworthiness on a continuing basis through management authorization, need to know, and continuous evaluation. Consideration must be given to assessing the mechanisms and controls used by the external entity to store, process, communicate, and exchange information to ensure it meets the organization's minimum security requirements.

Other considerations to be taken into account as part of the risk assessment effort should include the identification of the effect on the organization of the non-availability of externally provided products and services, or loss of data integrity, caused by inaccurate or misleading information. Processes that the external entity has established to identify and respond to security incidents should also be assessed to ensure that information about the incident is reported to the information owner should an incident take place. This process should include provisions for identifying conditions for suspending access in the event of a serious information breach. The assessment must address the legal, regulatory, and contract-related risks that may have an effect on external entity access to the organization's information. For example, the external party may need to implement controls to report security compliance, which have been mandated by government statute. The risk assessment should also evaluate how access by the external entity may affect other organizational elements, such as other business partners with whom information is already exchanged.

Addressing Security When Dealing with Customers

Information access by customers is subject to several special considerations. Organizations should ensure all identified security requirements are addressed before granting customers access to its information assets. Requirements for controlling customer access should include procedures for protecting assets from known vulnerabilities, mechanisms for ensuring compromises to organization information are reported, and restrictions on copying and disseminating information. Requirements may be documented in customer agreements, and rules of behavior, as well as warning messages and log-on banners.

Customers must clearly understand the service or product to be provided, and the purpose, requirements, and benefits for permitting their access to organization information. The organization should also ensure that customers are aware of its access control policy including access methods allowed (on-site or off-site, wired or wireless, physical or logical, etc.) and how customers are to control log-on credentials. There must be an explicit customer authorization process in place to regulate and control user access and assignment of privileges. Customers must be made to understand, preferably by signing a statement, that they are not permitted access to any information asset to which they are not specifically authorized. Organizations must also implement a process for revocation of customer access and disconnection of system interconnections in the event of a breach or violation. Customers must be aware of the organization's right to monitor and revoke as necessary any activity related to its information.

Reporting, notification, and investigation of data integrity issues, security incidents, and security breaches must be documented to guide customer actions.

Responsibilities of both the organization and the customer should also be made known to customers, including responsibilities for legal matters and protection of intellectual property.

Third-Party Agreements

All relevant security requirements should be covered in agreements with third parties that involve accessing, processing, communicating, or managing organization information or information assets. Third-party agreements must leave no room for misunderstanding between the organization and the third party. Consequently, organizations should consider the following items identified in ISO 27002 for inclusion in third-party agreements.

- Reference to and applicability of the information security policy to the third-party arrangement
- Identification of controls to ensure that assets are properly protected to include procedures for the security of hardware and software, physical security, protection against malware, compromise identification, return or destruction of information and assets when no longer required, protection of confidentiality, integrity and availability, and restrictions on information copying and disclosing information and use of confidentiality agreements
- User and administrator training and their awareness of information security responsibilities and issues
- Personnel management (assignment, transfer, and termination)
- Hardware and software installation and maintenance responsibilities
- Change management process
- Access control policy, including reasons, requirements, and benefits of third-party access; approved access methods, and the control and use of unique identifiers such as user IDs and passwords; authorization process for user access and privileges; requirements for maintenance of an authorized user's list specifying services, rights, and privileges; statement that all access that is not explicitly authorized is forbidden; and an access/connection revocation process
- Provisions for reporting and responding to information security incidents and violations of the third-party agreement
- Identification of the product or service to be provided
- Description of the information to be made available along with its security classification
- Expected level of service and definition of unacceptable levels of service
- Definition of verifiable performance measures and how they will be monitored and reported
- Stipulation of the organization's right to monitor, and revoke, any activity related to its information assets

- The right of the organization to conduct inspections and audits of activities related the agreement, through the use of independent auditors, following directions specified by the organization
- An escalation process for resolving identified problems
- Measures for ensuring service continuity according to the organization's operational priorities
- Specification of the liabilities of both parties to the agreement
- Responsibilities for meeting legal requirements such as data protection legislation
- Intellectual property rights, copyrights, and protection of collaborative work
- Control of subcontractor use of organization information
- Conditions for renegotiation and termination of the agreements

In addition to the third-party agreement itself, risks, security controls, and specific requirements can be detailed in an accompanying security management plan to ensure a clear definition of security responsibilities and how the organization's information will be protected.

Summary

Organizations can greatly improve their ability to secure information and information assets by establishing an effective information security function tailored according to the business needs for managing information security across the organization. An effective information security function significantly improves the organization's capability to implement, maintain, monitor, and improve security, and to be able to do so in a manner that is consistent with its organizational culture, mission, risk appetite, and priorities. To optimize organization-wide information security efforts, all levels of organization management must render the program visible support and commitment, including the timely provision of resources necessary to carry out information security activities. Finally, the information security function moving forward with solid management backing will be able to ensure that information security management requirements are properly identified and implemented, and that the performance of information security management activities is monitored and measured for adequacy and effectiveness.

Chapter 3

Cryptology

Maria Dailey

Contents

> There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government.
>
> **—Bruce Schneier**

Introduction

Through the centuries, the need for information protection persists. Humans are combative creatures—ritually engaging in warfare among one another. Combat has evolved from hand-to-hand to modern warfare, or cyber warfare. Combat is a combination of attack and defense, the latter of which has gained popularity with technological advances. Protecting sensitive data is critical to preserving trade secrets, government communications, or military strategies. Protection is achieved in part through the use of cryptology—more specifically, encryption. Cryptology is vital for everyday use in today's cyber society; online shopping and banking, ATM usage, and digital media all require encryption protection to avoid abuse. Unfortunately, many of today's systems lack appropriate protection—passwords and authentication requirements are not protected themselves, either through encryption or encrypted databases. This leaves sensitive information vulnerable to unauthorized, prying eyes. Cryptology is by no means a novel concept; it has existed since the beginning of sensitive communication.

Cryptology is "the science of keeping secrets secret" (Delfs and Knebl 2007). Cryptology is the study of encrypting algorithms and the art of creating and solving such algorithms, and is composed of both cryptography and cryptanalysis. Cryptography is the art or science of cipher systems used for protection information. The term originates from the Greek *kryptos* meaning "hidden," and *graphia*, meaning "writing." Cryptography protects sensitive information, identifies corruption or unauthorized access, and tries to compromise between expense and time consumption.

Cryptography has four basic purposes: (1) confidentiality, (2) authentication, (3) integrity, and (4) nonrepudiation. Confidentiality keeps information secret from unauthorized use. Authentication is the corroboration of an entity's identity, achieved through initial identification between communicators. Integrity assures that the message was not illegitimately altered during transmission or during storage and retrieval. Nonrepudiation guarantees that the sender will not deny previous commitments or actions unless they admit the cryptographic signing key has been compromised. Cryptanalysis is the practice of breaking ciphers, or decrypting messages without the key, to discover the original form of the message.

The most common use of cryptography is safe transfer of information across communication systems without compromising the integrity or authenticity of the message. Someone wishes to send a message, which begins as *plaintext*. Plaintext is the original, humanly readable form of a message, which is then *encrypted*. This could be text, numerical data, a program, or any other message form (Delfs and Knebl 2007). When plaintext is encrypted, or enciphered, the original message is obscured using an algorithm or pattern only known to the sender and authorized recipient(s). Encryption must be reversible; if not, the masked message is rendered useless to anyone. The algorithm or pattern is known as the *cipher*. A cipher is used to disguise information, making it immediately unintelligible. Once encrypted, the message is referred to as *ciphertext*, and is only readable when the *cipher key* is used in conjunction with the decrypting algorithm. A key, which is a secret sequence used by authorized correspondents, does not give immediate access to the plaintext. The encryption key is not always the same as the decrypting key. *Decrypting*, or deciphering, requires that the cipher inverse be performed on the ciphertext to reveal the plaintext. Preferably, only authorized persons know the decrypting algorithm. This relies on the complexity of the applied cipher. If the key is discovered, either through poor management or faulty circle of trust, the cipher is compromised. Protecting the key, and to whom it is known, is crucial to ensuring the authenticity, integrity, and confidentiality of the transmitted message. An element, known as the *work factor*, often forgotten, is not *if* the algorithm can be broken, but how *long* until it is broken. The most strategic mindset when encrypting is creating a cipher that would take an unreasonable amount of time to solve.

History

Cryptography is an ancient art, going as far back as the Egyptians. Cryptography was originally used as a "tool to protect national secrets and strategies" (Menezes et al. 1997). Two additional ancient ciphers are the Spartan scytale and the Caesar cipher. In the Spartan scytale, a segment of parchment is wrapped around a cylinder of certain radius and the message is written lengthwise. The recipient must have a cylinder of equal radius to decrypt. The Caesar cipher is a "classical" cipher, using a simple shift of the plaintext alphabet.

In the early twentieth century, cryptography broadened its horizons. No longer did it use arbitrary characters or scrambled letters, but it became more mathematical. Cryptography is now considered more of a science than an art—"cryptographic protocols for securely proving… identity online… or signing binding digital contracts are now at least as important as ciphers" (Talbot and Welsh 2006). One of the first among the more complicated cryptosystems used an electronic machine known as the Enigma rotor machine. Enigma, used by the Germans in World War II, applied a substitution cipher multiple times per message.

In the mid-twentieth century, there was a demand from the private sector with the advent of the Internet. As more users access the Internet, the need for digital information security is greater. This massive increase in public use of cryptography has led to the "standardization" of cryptography in a scientific sense. Developers must take care that the mathematics used in newer cryptosystems remains unsolvable;

currently, many systems are secure, but rely on plausible assumptions that may one day be discovered. The standardization and mathematical focus of modern cryptosystems unfortunately shares the same issue suffered by earlier ciphers. One of the better-known modern encrypting systems is the Data Encryption Standard (DES), which was adopted in 1977 by the United States. This was shortly followed by public key encryption, which branched into the RSA scheme and digital signatures. The concept of public key encryption was unintentionally introduced in 1976. Two years later, a practical application was developed, known as the RSA algorithm (named after its creators, Rivest, Shamir, and Adleman). RSA is based on factoring large integers. The Enigma rotor machine, DES, and RSA schemes are examples of modern ciphers.

Formatting

Universally, plaintext is written in lowercase when explaining applied cryptography. Ciphertext is written in all capitals. Keys or keywords are also always written in capitals.

When referring to those who use cryptosystems, certain names typically are used as the placeholders. Rather than referring to the sender as “Party A” and the recipient as “Party B,” Party A would be Alice and Party B would be Bob. Alice and Bob are always trying to communicate. Each associate communicating continues alphabetically, for example, Charlie and David want to speak with Alice and Bob. Eve is an eavesdropper, who does not have authorized access to the message. Eve is a passive listener; she does not modify the message. Mallory is a malicious attacker and modifies, sends her own, or repeats previous messages. Victor is a verifying agent who demonstrates that the intended transaction was successfully executed.

Kerckhoff’s Six Principles

In 1883, Auguste Kerckhoff published journal articles titled “La Cryptographie Militaire” (Petitcolas 2011). These articles articulated the importance of the following principles, which provide the fundamentals necessary to develop a cryptosystem. There are six principles, as follows:

1. The system must be practically or mathematically undecipherable.
2. The system is not required to be secret and should be able to fall in enemy hands.
3. The key must be communicable and retained without effort, and changeable at the will of the correspondents.
4. The system must be compatible with the communication channel.
5. The system must be portable and not require functioning by multiple people.
6. The system must be easy, requiring minimal knowledge of the system rules.

Types of Ciphers

There are two generations of encrypting methods; classical and modern. Classical ciphers are those that were historically used, like the scytale and Caesar's, but became impractical either resulting from popular use or advances in technology. Modern ciphers consist of substitution or transposition ciphers. The time it would now take to decrypt classical ciphers is miniscule compared with more complex, modern ciphers. Classical ciphers use an alphabet of letters, implemented using simple math. The math, being simple, proved to be a key weakness. Classical ciphers can be broken using brute force attacks or frequency analysis. Brute force is a standard attack, running possible keys with a decrypting algorithm until the plaintext is exposed. Frequency analysis studies how often certain letters or letter groups appear in ciphertext. This method relies on the varying frequencies to uncover certain letters, and eventually break the entire cipher.

Modern cryptography became more of a science in concurrence with technological advances. It grew to envelop more than just encryption, but emphasized the importance of "digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, digital cash, and more," addressing issues arising externally or internally (Vacca 2010).

Another difference between modern and classical cryptography is the user profile. Previously, cryptography was officially used by military or government figures. Today, cryptography is used by everyone aware and desiring.

Modern ciphers are typically divided into two criteria: the key type used and the data input type. When referring to key types, modern ciphers branch into symmetric (private key cryptography) or asymmetric (public key cryptography). Symmetric key algorithms use the same key for encryption and decryption. Asymmetric key algorithms use two different keys; one for encrypting and another for decrypting. Asymmetric ciphers, introduced in the 1970s, nearly solved the dilemma of ensuring authenticity and nonrepudiation. An example of an asymmetric cipher is the RSA scheme. Data input ciphers branch into block and stream ciphers. Blocks ciphers encrypt blocks of data of fixed size. Stream ciphers encrypt continuous strands of data using pseudorandom numeric or alphabetic keystreams.

Substitution Ciphers

When one thinks of encrypting, the first technique to come to mind is scrambling the message. Substitution ciphers are the most basic type of encryption. There are two types of substitution ciphers, which replace characters with other characters using a single rule (monoalphabetic) or groups of rules (polyalphabetic).

Monoalphabetic Substitution Ciphers

Monoalphabetic substitutions include the Caesar, Atbash, and Keyword ciphers. A prime example of a substitution cipher is the Caesar shift cipher, which is typically a three-character shift. Depending on how large the shift, either by subtraction or addition, the alphabet will be offset by that much. For instance, a three-character addition shift would look like Figure 3.1. This shift would change the plaintext “purple” into the ciphertext “MROMIB.”

If the shift was a three-character subtraction, it would look like Figure 3.2. The plaintext message “purple” would then become ciphertext “SXUSOH.”

The Atbash cipher flips the entire alphabet back on itself; the plaintext alphabet is “A–Z” and the ciphertext alphabet is “Z–A,” shown below in Figure 3.3. The Atbash cipher would obscure the plaintext “purple” as “KFIKOV.”

Plaintext	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Ciphertext	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Plaintext	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Ciphertext	K	L	M	N	O	P	Q	R	S	T	U	V	W

Figure 3.1 Example of the Caesar cipher, three-character addition shift.

Plaintext	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P

Plaintext	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figure 3.2 Example of the Caesar cipher, three-character subtraction shift.

Plaintext	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Ciphertext	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Plaintext	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Ciphertext	M	L	K	J	I	H	G	F	E	D	C	B	A

Figure 3.3 Example of the Atbash cipher.

Plaintext	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
Ciphertext	H	E	A	D	Y	B	C	F	G	I	J	K	L

Plaintext	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Ciphertext	M	N	O	P	Q	R	S	T	U	V	W	X	Z

Figure 3.4 Example of the Keyword cipher.

Another cipher, the Keyword cipher establishes a keyword such as "HEADY." This begins the ciphertext alphabet, and the rest is completed using the remaining letters in alphabetic order. This can be seen in Figure 3.4, using "HEADY" as the keyword. The Keyword cipher changes the plaintext "purple" to "OTQOKY."

Polyalphabetic Substitution Ciphers

Polyalphabetic substitutions are ciphers using multiple substitution alphabets. The Vigenère cipher is the most famous of this genre, introduced in the sixteenth century by Blaise de Vigenère. The Vigenère cipher uses the keyword to encrypt a message using relations. A barebones explanation of a Vigenère cipher is that it encrypts plaintext by using a series of Caesar ciphers, based on the keyword. It is easy to apply, and has the deceitful appearance of incredible complexity. The keyword is written as many times as necessary above the plaintext message, as depicted in Figure 3.5.

Using the Vigenère square, depicted in Figure 3.6, one will use a letter from the plaintext and its associated keyword letter. Plaintext letters are listed on the top, creating columns, which intersect with the keyword alphabet along the left side of the square, creating rows. The letter found at the intersection of these two letters is the cipher letter used to encrypt the message. The beginning of the plaintext "O" and keyword letter "K" intersect at ciphertext letter "Y." Therefore, "once upon a time" would become "YVPKM ZWAGL SUR."

The 25 variations of the Caesar cipher (shifts 0–25) are contained in the square. Each row is a single shift to the right from the row or letter preceding. Therefore, the

Keyword	K	I	N	G	S	K	I	N	G	S	K	I	N
Plaintext	o	n	c	e	u	p	o	n	a	t	i	m	e

Figure 3.5 Example of the first step in Vigenère encryption.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 3.6 The Vigenère square. Each row corresponds to a Caesar cipher. The first row shift is zero, the second is a shift of 1, and the last shift is 25.

first row, labeled "A," is a shift of one. Row "X" is a shift of 23. It is important that the intended receiver knows the keyword used to encrypt the message to reverse the ciphertext. To decrypt the ciphertext using the known keyword, do the reverse of the above steps. First, write the keyword above the ciphertext, demonstrated in Figure 3.7. Then, find the first letter of the keyword, in this instance "K," and follow the column down until the associated ciphertext letter is encountered, which is "Y." Follow the row to the left and the letter found on the outmost column is the plaintext letter, being "O." Continue this process until the message is decrypted.

The cipher was broken by Prussian Major Kasiski in 1863 by finding the keyword length and dividing the message into that number of blocks, or cryptograms, based on repeated letter sequences. The distance between these common patterns

Keyword	K	I	N	G	S	K	I	N	G	S	K	I	N
Ciphertext	Y	V	P	K	M	Z	W	A	G	L	S	U	R
Plaintext	O	N	C	E	U	P	O	N	A	T	I	M	E

Figure 3.7 Example of the initial step, followed by the result, of decrypting using a Vigenère square.

is counted, which clues the attacker into the possible keyword length. Sometimes, the keyword length is actually a factor of the distance counted. The ciphertext is then split into the deduced keyword length, called cryptograms. A frequency analysis is then applied to each cryptogram to determine the specific keyword letter used. This method is commonly referred to as the Kasiski/Kerckhoff method. If the frequency analysis was applied before creating cryptograms, the bar graph would appear flattened in comparison to a monoalphabetic cipher. This is because each letter is encrypted with a different shift. The flatter a frequency analysis graph, the stronger the cipher. One way to apply a Vigenère square's fullest potential is to choose a keyword equal to the message length. Although one of the strengths relies on the square's ability to encrypt the same letter or series of letters in various ways throughout the same message, it is inevitable that of those variations, they will repeat later in the message.

Transposition Ciphers

The second major family of substitution is transposition ciphers. Rather simple and easy to crack, these ciphers use the same letters as the plaintext but reorganize them until the message is scrambled. This is achieved by applying a permutation to single characters or character blocks. Permutation determines the specific order for a finite group of characters. A sender cannot scramble the message without knowing the reverse; hence, the need for order-specific reorganization. The Spartan scytale is an example of a simple form of transposition. Using a cylinder, a piece of parchment was wrapped around it and the message written lengthwise. When unwound, the message was scrambled. The intended recipient would have a cylinder of exact diameter and wrap it with the parchment to decrypt the message. The permutation in this case would be related to the diameter of the cylinder.

The most basic transposition cipher is the rail fence cipher. The plaintext is split onto several "rails" or rows, each letter alternating from topmost row and down. The ciphertext is recorded by writing the letters through one row, then moving to the next and repeating. An example would be the plaintext "walking through the park one time." Figure 3.8 demonstrates the rail fence cipher using this plaintext.

The ciphertext would be written as "WLIGHOGTEAKNTMAKNTRUHH-PROEIE." Rail fence does not always require the topmost rail be furthest left. If

W	L	I	G	H	O	G	T	E	A	K	N	T	M
A	K	N	T	R	U	H	H	P	R	O	E	I	E

Figure 3.8 Example of the rail fence cipher with two "rails."

each rail is slightly offset from the other, where the left-most character is on the bottom rail, as seen in Figure 3.9, the ciphertext is still recorded the same (beginning on the top row).

Another type of transposition cipher is the columnar transposition cipher. The number of columns is equal to the key or keyword length. The plaintext is written lengthwise across the columns, creating a new row when each columnar slot is filled. Each column is then rearranged according to the chosen cipher pattern. If a numerical key is used, the numbers are out of order for plaintext, then rearranged to create the ciphertext (Figure 3.10). If a word or phrase is used as the keyword, then the associated number placement of the letter determines the order of the columns for encrypting (Figure 3.11). When a key or keyword is applied once, this is known as a single columnar transposition. If applied twice, it is known as a double columnar transposition, and so on. Sometimes, if a message falls short, as the example text provided does, filler text is added such as "XX" or other characters. However, filler text is a security risk. Incomplete rows make it more difficult to decrypt the message without the key.

W	L	I	G	H	O	G	T	E	A	K	N	T	M
A	K	N	T	R	U	H	H	P	R	O	E	I	E

Figure 3.9 Example of the rail fence cipher with two "rails," offset so the bottom rail begins the ciphertext.

1	**2**	**3**	**4**	**5**		**4**	**2**	**5**	**3**	**1**
t	r	y	r	e		R	R	E	Y	T
a	d	i	n	g		N	D	G	I	A
t	h	i	s	n		S	H	N	I	T
o	w						W			O

Figure 3.10 Example of the columnar transposition cipher using a numerical key.

K	I	N	G	L	Y
10	**8**	**13**	**6**	**11**	**24**
t	r	y	r	e	a
d	i	n	g	t	h
i	s	n	o	w	

G	I	K	L	N	Y
6	**8**	**10**	**11**	**13**	**24**
r	r	t	e	y	a
g	i	d	t	n	h
o	s	i	w	n	

Figure 3.11 Example of the columnar transposition cipher using a keyword.

In this example, the plaintext "try reading this now" is written lengthwise across five columns. Above each column is a number, the left being the lowest and the right being the highest. The selected key is 42531. When encrypting, the columns are labeled as such and the associated letters found in each column organized accordingly. To write the ciphertext, copy each column, moving left to right. The encrypted message is broken into groups of five cryptograms consisting of five characters. The ciphertext in this example would become "RNSRD HWEGN YIITA TO." Now, the keyword "KINGLY" will be used in place of numbers. Remember, when encrypting with a keyword in columnar transposition, the letter's placement in the alphabet must be written down. Figure 3.12 lists the alphabet with its associated numbers. Using keyword "KINGLY," the message "try reading this now" will be encrypted.

The alphabetic numbering lets the sender organize the columns for encrypting by the earliest letter to the latest. The columns are now reorganized into "GIKLNY." This encrypts "try reading this now" into "RGORI STDIE TWYNN AH."

Decrypting this ciphertext requires finding the sum of characters in the message to determine the number of characters found in the last row, before encryption. The message is 17 characters long. Authorized recipients know the keyword length, which is six characters, and would be able to determine the last column only had two characters. This is an irregular columnar transposition, whereas even distribution of the rows would be regular. Decryption without knowledge of the

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 3.12 The alphabet, numbered 0 to 25.

key is rather simple with columnar transpositions. Trying different permutations through brute force will eventually yield plaintext.

Cryptographic Keys

More complex ciphers use secret keys that control long sequences of intricate substitutions and transpositions. This partnership between simple ciphers creates a powerful and modern form of communication security. In one form of encryption, the key is secretly exchanged between correspondents before message transaction proceeds; in another, some keys are made public and others are kept private.

Private Key

Private, or secret key encryption, often referred to as a symmetric key, is a class of algorithm that uses a single key to encrypt or decrypt messages. The key is confidential information used when the involved parties wish to communicate with one another. For maximum security, each pair of correspondents has a separate key; it is vital that both parties keep the key secret. The sender encrypts the message using the key before transmitting it to the recipient. The recipient uses the same key as the sender to decrypt the message. The key acts as the authentication service, distinguishing correspondents from other parties, malicious or otherwise. Messages are typically sent over a public channel, and eavesdropping is a realistic threat. If the key is known, the messages' integrity is compromised. Correspondents must establish a secure manner of sharing the key; private key encryption relies solely on the protection of the key for success (Figure 3.13).

Private key encryption is commonly used for session keys in security protocols. A session key is randomly generated for communication between a computer and its user, or between two computers. Every session of communication generates a

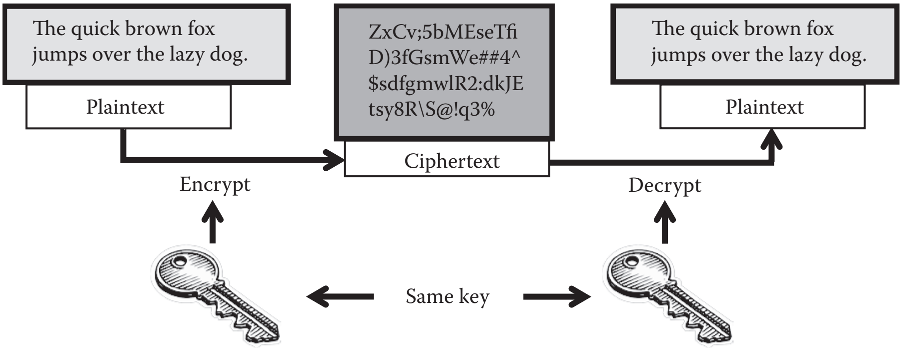


Figure 3.13 Example of a private key.

new session key. Sometimes, each message may use a new session key. Private key encryption is also used for bulk encryption for continuous data, such as e-mail.

Private key encryption is divided into stream ciphers and block ciphers. Stream ciphers operate on continuous data that arrives in "real time;" information is encrypted a bit at a time, as opposed to block ciphers. Block ciphers break plaintext into blocks. These fixed-length blocks are then encrypted a block at a time. A key of fixed length is applied multiple times to the series of blocks. Block ciphers are typically used when securing computers. A well-known type of block cipher is the DES algorithm, which is a type of private key encryption. An updated and more reliable block cipher used today is the Advanced Encryption Standard (AES).

DES Algorithm

DES is a nonlinear block cipher. The plaintext is broken into 64-bit blocks and encrypted using 56-bit key and 8 parity bits, totaling 64 bits. The 8 parity bits act as verification that the key was not modified without authorization. Generating the key requires breaking the 56 bits into 7-bit segments, which are moved into 8-bit-long slots. Parity bits are set to either 0 or 1. Each parity bit is assigned so that each octet has an odd total number of 1's. Encryption is achieved through dividing the blocks in a left (*L*) and right (*R*) parts and applying a series of permutations and substitutions 16 times.

DES originally was IBM's Lucifer in 1973, an answer to the National Bureau of Standards' (NBS) request for an encryption algorithm that meets several criteria: high security level, small key for encryption and decryption, easily understood, independent of algorithm confidentiality, adaptable, and efficient and exportable. Lucifer was modified in 1976 and became DES, which was adopted in 1977 and standardized by the American National Standards Institute (ANSI). In 1987, the National Security Agency (NSA) threatened to decertify DES, but DES reapplied in 1999 as 3DES/TDEA. 3DES, or Triple DES, is a partial successor to DES, using three different keys totaling as a 168-bit key. DES became insecure in the industry whereas 3DES is too slow. DES is insecure because its key length is relatively short, and 3DES is insecure because of a vulnerability enabling malicious users to modify the key length. This inherently reduces the time necessary for cryptanalysis.

AES Algorithm

AES resulted from a worldwide competition that started in 1997 under the sponsorship of the National Institute of Standards and Technology (NIST). The victor was determined after 3 years of analysis of the submitted algorithms. An important attribute that the NIST outlined was that the new encryption algorithm would have a public key strong enough to protect government information into the following century. Two Belgian cryptologists, Vincent Rijmen and Joan Daemen, created an algorithm and submitted it under the name Rijndael (a combination of its creators' surnames). In 2000, the algorithm, which would later be known as AES, was announced as the winner. In 2003, the NSA determined that AES was secure enough to protect sensitive information.

AES is an iterative block cipher based on substitutions and permutations. The fixed blocks are each 128 bits long, or 16 bytes. This is double the length used by DES, increasing the number of possible blocks by 2^{64}. This algorithm uses key lengths of 128, 192, or 256 bits. The increasing length of each key offers a greater plethora of potential combinations, increasing the complexity of the cipher. Before implementing encryption, each block is divided into a four-by-four array, each 8 bits long. Each time an array is processed, it is treated in substitution or permutation boxes, known as S-boxes or P-boxes, respectively. The S-box substitutes the arrays for one another. A single bit change in the input causes multiple bit changes in the output. The P-box shuffles the input to create an output. These are performed in rounds, consisting of four transformations. There are two inputs per round: the array and a round key. The round key is generated using the cipher key and key expansion routine. This process creates the ciphertext. The inverse of the applied algorithm unveils the plaintext.

A weakness of DES is that its security was designed for hardware-based protection. AES is more versatile, effectively operating on software and hardware. The broad application of AES is not the only benefit of the updated encryption algorithm; AES is faster and more secure than DES or DES' derivatives such as Triple DES. Despite these benefits, AES remains unused by certain organizations or companies using legacy software and equipment like DES. As technology advances and older systems become incompatible with newer software and equipment, DES will become obsolete. Without AES, different encryption algorithms are necessary to protect specific programs. AES' increased compatibility and economic benefits simplify the encryption of organization equipment and software through standardization.

Public Key Encryption

The first public key encryption cryptosystem was proposed by Ralph Merkle in 1974, and introduced two years later, in 1976, by Professor Martin Hellman from Stanford University and Whitfield Diffie, then at Northern Telecom (Bosworth et al. 2009). Public key encryption uses two separate keys to encrypt and decrypt. Another name for public key encryption is asymmetric encryption. Unlike private key encryption, public key encryption uses one key to encrypt and another to decrypt. One key is public and the other, the private key, is known only to the originator of the ciphertext. Each correspondent has a public key and a private key; what is encrypted using one key is decrypted using the other key. The public key of either correspondent is widely available whereas the private key is available only to the owner of the public/private key pair. When encrypting a message so that only the intended recipient can decrypt it, the sender uses the recipient's public key and the recipient decrypts it using the corresponding private key. When encrypting a message so that anyone can authenticate its origin, the sender uses his or her own private key and recipients use the corresponding public key to decrypt the ciphertext.

Public key encryption enables secure electronic business transactions, applied through keys and certificates. This cryptosystem supports confidentiality, access control, integrity, authentication, and nonrepudiation services. Both keys are generated simultaneously as large prime numbers. A prime number is an integer which has no integral factors apart from the numeral one and itself. In this instance, the longer the key, the more secure the correspondence will be.

For example, to authenticate a message to Bob, Alice encrypts the message using her own private key before sending to Bob. Bob then decrypts the ciphertext using Alice's public key. Figure 3.14 demonstrates the process when a message from Alice is received by Bob. This process also verifies the integrity of the transmitted message because any change in the ciphertext during transmission makes it impossible to decrypt the message using public key encryption.

Figure 3.15 shows how to encrypt a message so that only the intended recipient can decrypt it. Thus, Alice encrypts a message for Bob to receive by encrypting it using Bob's public key. Bob decrypts the ciphertext using his private key.

Public key encryption provides a solution for the private key weakness. This algorithm is more secure than private key encryption, eliminating the key exchange problem. Private key encryption requires a separate, secure channel to exchange the encrypting and decrypting key. Public key encryption does not require this separate channel. In addition, the private key system suffers from the *combinatorial explosion*, which increases the number of key pairs required for n correspondents as a function of $n(n - 1)/2$ or as approximately n^2 for large numbers of correspondents. A group of 10 correspondents needs 45 key pairs for security, but a group of 100

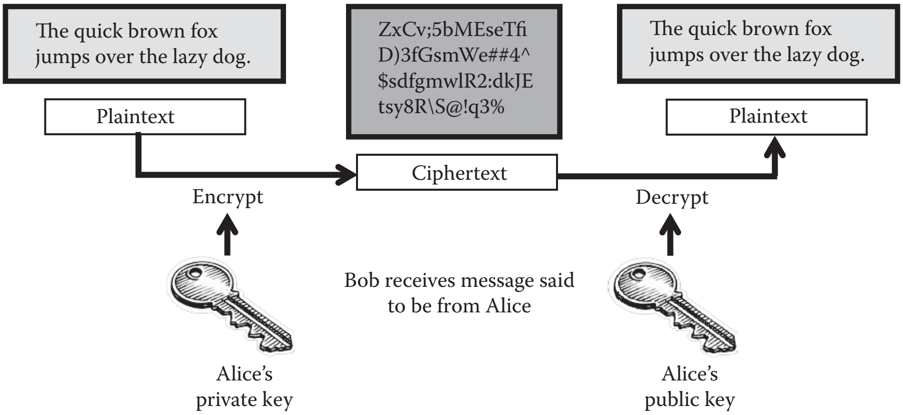


Figure 3.14 Public key encryption: Bob receives Alice's encrypted message and uses her public key for decryption.

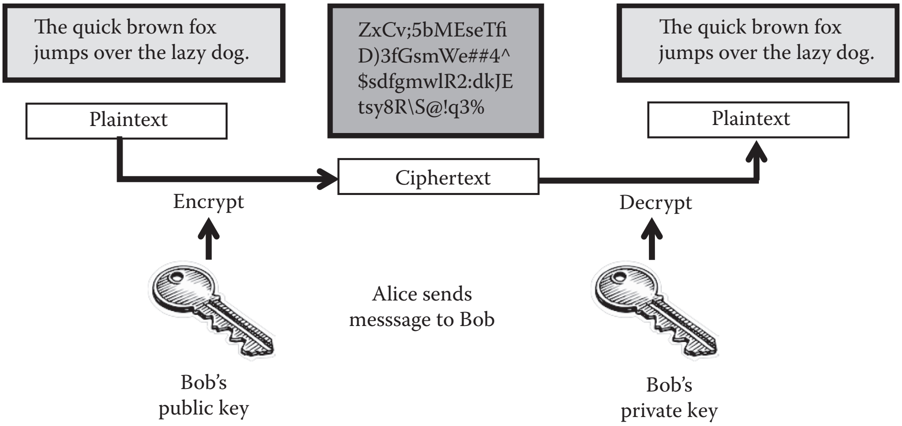

The quick brown fox jumps over the lazy dog.
Plaintext
ZxCv;5bMEseTfi D)3fGsmWe##4^ $sdfgmwlR2:dkJE tsy8R\S@!q3%
Ciphertext
The quick brown fox jumps over the lazy dog.
Plaintext
Encrypt
Decrypt
Alice sends messsage to Bob
Bob's public key
Bob's private key

Figure 3.15 Public key: Alice encrypts a message for Bob using his public key. He decrypts using his private key.

needs 4950 key pairs and a group of 1000 needs 499,500 pairs. In contrast, PKC users need *n* key pairs, so 1000 users need 1000 key pairs.

Modular Arithmetic

Public key encryption was made possible by the Diffie–Hellman system, which uses modular arithmetic. Modular arithmetic differs from typical arithmetic by executing operations in a circle rather than in a line. This is also known as congruence arithmetic. There is a fixed amount of numbers, which is less than the fixed maximum number, known as the modulus. These integers are cycled through. Every time the largest number is passed, one starts again with the first value. Oftentimes, modular arithmetic is compared with a clock. There are 24 hours in the day, but only 12 hours are shown on a clock. The first rotation is daytime and the second is the evening. A clock is mod-12 arithmetic, meaning the available integers are 0 to 11, zero being the first integer, standing in the place of 12. Figure 3.16 depicts a mod-12 clock, where zero stands in for 12.

If an e-mail said there was a meeting at 1100, that would mean that it was at eleven o'clock, presented in the 24-hour format. Similarly, if someone had a meeting at 1400 but was unfamiliar with the 24-hour format, they would simply "wrap" around the 12-hour clock and find the remainder, which would present the time in another form. Written out in modular arithmetic, this problem would look like: 14 (mod 12).

1. Meeting at 1400
2. 1400 – 1200 = 200
3. Rotate forward on the 12-hour clock two spots
4. The meeting is at 2:00 pm

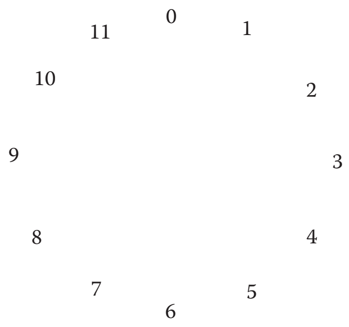


Figure 3.16 A clock demonstrates modular arithmetic.

The steps above simplify the process. Step 2 would actually be written as 14 (mod 12). Using a calculator, this function would be done by dividing 14 by 12, which equals 1.167. Subtract 1 from 1.167 to get 0.167, which is then multiplied by the modulus, 12. This provides the remainder, which is 2. Therefore, 14 (mod 12) equals, or is congruent to, 2. Smaller values are easier to analyze, but when presented with a larger value such as 107 (mod 12), Step 2's method becomes impractical. Using the method aforementioned, one will find that 107 (mod 12) is congruent to 11.

1. 107 (mod 12)
2. 107/12 = 8.9167
3. 8.9167 – 8 = 0.9167
4. 0.9167 * 12 = 11
5. 107 (mod 12) = 11

The modulus equals the total integers; there are 12 hours on a clock; therefore, it is modulus 12, or mod 12. The array of integers derived from the modulus starts with zero and ends one integer less than the modulus. A 12-hour clock would have an array from 0 to 11, which looks like this: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.

Diffie–Hellman System

The Diffie–Hellman key exchange is based on the premise that two correspondents, Alice and Bob, wish to communicate a secret number, but must do so on an insecure channel. An unauthorized user, Eve, is trying to intercept the message over the unsafe channel. If Eve obtains the message containing the key, all integrity and confidentiality is lost. This issue is resolved by masking the key using modular arithmetic. Alice and Bob achieve secrecy by agreeing on a large prime number, p, and a base number, n. Alice will choose a personal, private value, a, which remains unknown to Bob. Bob will generate a secret value only known to himself, b. It is important that a and b are less than p. Alice and Bob's respective secret keys should be relatively prime to *n*, meaning that neither shares common factors with *n*. Alice's public value is n^a mod *p* and Bob's is n^b mod *p*. The two correspondents exchange their public values, so that both parties now know both. Alice will compute $n^{ab} = (n^b)^a$ mod *p*. Bob will compute $n^{ba} = (n^a)^b$ mod *p*. Once both algorithms are computed, each party will have the same number. Alice and Bob are now able to privately communicate on the insecure network.

Future of Cryptography: Quantum Cryptography

The further cryptology advances, evolving and becoming more secure each decade, the greater advantage cryptographers have over cryptanalysts. A technique currently in development is quantum cryptography. Depending on the chosen polarization, Alice can send a unique public key to Bob, which can change per message. Currently, quantum cryptography is theoretically unbreakable. Although modern computers gain speed with emerging technologies, the fundamental functions do not change. Computer computation is currently based on bits, which are represented by "0" or "1," never both states at once. Data is stored in bytes, which is equivalent to eight bits. This two-state system is known as binary. Binary systems are base 2 rather than base 10 used in the decimal system.

Quantum refers to the "smallest amount of a physical radiation" capable of angular momentum, such as particles, atoms, and energy (American Heritage Science Dictionary 2013, "Quantum"). Richard Feynman, an American physicist, introduced a computer capable of effectively combining quantum mechanics (Bone and Castro 1997). Quantum computers use quantum bits, or qubits, rather than standard bits. Qubits represent the atoms and their included components: ions, photons, and electrons. Photons begin the process of generating a key for secure transmission, and are translated into binary code. Each rotation of the photon represents either a one or zero, which are the only components of a binary system. Quantum cryptography is based on photon physics, which focuses on the polarization of the photon, based on the theory that this angular momentum can occur on atomic and subatomic levels, defying all modern definitions of the law of physics (Jenkins 1996). This defines the main difference between quantum and modern computers; a qubit can assume either a "0," "1" or both states simultaneously. For example, photons with a vertical spin can be assigned "0" and horizontally spinning photons are assigned "1." When a qubit is both "0" and "1," it exists in its coherent state, achieving quantum parallelism. This is the attribute which makes quantum computers exponentially more powerful than modern computers. Any operation applied to a coherent state qubit would affect both properties at once, producing two separate outputs.

The same aspect setting quantum beyond and apart from modern computer is very hard to control. Decoherence requires measuring qubit outputs once an operation is executed. When one tries to discover if the qubit outputs are either "0" or "1," simply interacting with the output can impede on accurately reading its value. An indirect manner of measuring must be implemented and is yet to be discovered. Quantum computing and cryptography has not yet taken because algorithms necessary to harness quantum parallelism do not exist today. Peter Shor and Lov Grover, both of Bell Laboratories, have made advances with their respective algorithms (Bosworth et al. 2009, p. 7.40). Other advancements have come in the form of entanglement, a possible solution for measuring qubit outputs. Entanglement states that when certain requirements are met involving more than two particles, they entangle. One particle is able to communicate with its partner, revealing the opposite of its value. This concept is still in development, with most success found when applied by the Los Alamos National Laboratory and the Massachusetts Institute of Technology. Using nuclear magnetic resonance (NMR), scientists at these facilities discovered that spreading out the qubit increases the difficulty of identifying outputs (Bosworth et al. 2009, p. 7.41). This technology enables scientists to manipulate the spinning of a nucleus.

Despite scientists' best efforts and commitment toward making quantum computing and cryptography possible, the practical application of this method is possibly decades away. There are still many obstacles to overcome, especially the matter of measuring coherent state qubit outputs. Once this is discovered, the issue of a computer powerful enough to efficiently handle large-scale computations still blocks the finished product. The question is not *if* quantum cryptography is possible, but *when* it will be accurate and reliable enough for application.

Cryptanalysis

There are many means by which to break a code. Some are orthodox whereas others are obvious but overlooked. These strategies range from "guess and check," to educated computations, and even personal interactions. Guess and check, or brute force attack, is used most often, especially with simpler cryptosystems like Caesar. Educated computations envelope frequency analysis, or the relation of characters used in ciphertext with the frequency of the implemented alphabets' individual characters in a section of text. Personal interactions include social engineering and man-in-the-middle attacks. Social engineering exploits human vulnerabilities—it is human nature to want to help others and be trusting. Attackers of this nature manipulate critical personnel to obtain sensitive information. Man-in-the-middle attacks are committed over communication channels between Alice and Bob to eavesdrop on keys exchanged for private and public cryptosystems. All of these methods are used in an attempt to break ciphers to reveal, alter, or intercept the hidden message.

Brute Force

Brute force decryption is a method of repetitious trial-and-error. This method is implemented until the key is revealed, or all possible options are exhausted. Brute force can be incredibly time-consuming, but is unfailing. In theory, this method can be applied to any cryptosystem. Whether or not this is practical depends on how long it will take to test every possible key. Key length determines the feasibility of this method. In a given amount of time, the key will be discovered. However, if the key is not found in this lifetime, or any lifetime soon to follow, it remains secure for the time being. As technology advances, computers will be able to process more information in less time, and keys that were secure in the twentieth century may not remain so by the twenty-third century. Time is a critical factor in assessing a cryptosystem's strength.

Frequency Analysis

Attackers are able to use ciphertext-only methods and letter frequency analysis on the encrypted messages. Ciphertext-only attacks are where the attacker only has access to the ciphertext. If any information is gathered about the plaintext, breaking the cipher becomes much easier. Frequency analysis is the study of letter or letter group frequencies in ciphertext. This analysis is based on the fact that in an alphabet, certain letters are used more frequently than others. In a section of English (e.g., a complete sentence), the most common letters to appear are in the following order: "ETAOIN." Following this sequence with the next highest frequency are "SHRDLU." The most common letter pairs of the English language are "TH," "ER," "ON," and "AN." Repeats of high frequency are "SS," "EE," "TT," and "FF."

Man-in-the-Middle Attack

Man-in-the-middle attacks are somewhat similar to social engineering attacks; the unauthorized user deceives the authorized parties into providing their respective keys. The attacker listens to the communication channel between Alice and Bob, who are about to exchange their keys for secure encryption. This is most commonly seen in private and public key cryptosystems. The attacker exchanges keys with each party, who are none the wiser. The authorized parties believe they have securely exchanged keys. When the key, which is known only to the attacker, is applied to the messages, the attacker can decrypt it and obtain sensitive information. To avoid this attack, a hash function is applied, which transforms longer character strands into short, fixed-length keys, therein masking the original key.

Summary

An ever-increasing necessity in today's world stems from the expanding use of e-commerce and other sensitive activities. The importance of securing general information or e-trade, as well as addresses and records, is critical for both business and personal interactions. This chapter covers many different methods, classified by the era in which they were most effective. As time went on, and cryptologists developed more complex cryptosystems, it became difficult to judge which was superior to another. The advances in technology in modern security have made this question easily measurable; the greatest advantages are had by cryptosystems with longer, obfuscated keys, and caretakers of the keys who are wary and cautious when exchanging sensitive information.

Cryptology will continue to be an essential practice in societies around the world. More activities are becoming digitized, such as banking, shopping, communication, and networking. Everyday life and organizations determining how nations are run all depend on secure communication and transaction channels. Cryptology is universally applied and will continue to develop and evolve to adapt to technological advances. No longer is cryptology restricted to the military, the economy, and the government; it is practical for everyone.

Terminology

Algorithm: a well-defined set of instructions for manipulating given variables

Cipher: a type of algorithm used to encrypt data, changing plaintext into ciphertext and irreversible without a key

Ciphertext: legible text in encrypted form, written in uppercase

Cryptanalysis: the art and science of breaking ciphers, decryption, through "unauthorized" means (unknown key)

Cryptography: the science of encrypting and decrypting messages, originating from the Greek terms *kryptos* ("hidden") and *graphia* ("writing")

Cryptology: the study of secure communications, formed from the Greek terms *kryptos* ("hidden") and *logos* ("word")

Cryptosystem: system for encrypting information

Decrypt: the process of unmasking the plaintext from the ciphertext (also decipher)

Encrypt: altering the plaintext using a keyword and specific algorithm so it becomes unintelligible to unauthorized parties, referred to as ciphertext (also encipher)

Key/keyword: a word or system for encrypting or decrypting a cipher

Plaintext: the original, readable message, which is encrypted

References

American Heritage Science Dictionary. (2013). *Quantum*. Retrieved November 14, 2011, from Dictionary.com: http://dictionary.reference.com/browse/quantum.

Bone, S., and Castro, M. (1997). *Introduction*. Retrieved November 20, 2011, from *A Brief History of Quantum Computing*: http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/.

Bosworth, S., Kabay, M. E., and Whyne, E. (2009). *Computer Security Handbook* (5th ed., vol. 1). Hoboken: John Wiley & Sons, Inc.

Delfs, H., and Knebl, H. (2007). *Introduction to Cryptography: Principles and Applications* (2nd ed.). New York: Springer.

Jenkins, S. (1996). *Some Basic Ideas About Quantum Mechanics*. Retrieved November 14, 2011, from University of Exeter: http://newton.ex.ac.uk/research/qsystems/people/jenkins/mbody/mbody2.html.

Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (1997). *Handbook of Applied Cryptography.* Boca Raton: CRC Press LLC.

Petitcolas, F. (2011). *La Cryptographie Militaire*. Retrieved December 19, 2011, from Fabien Petitcolas: http://petitcolas.net/fabien/kerckhoffs/.

Talbot, J., and Welsh, D. (2006). *Complexity and Cryptography: An Introduction.* Cambridge: Cambridge University Press.

Vacca, J. R. (2010). *Network and System Security.* Oxford: Elsevier Inc.

Chapter 4

Risk Management: The Facilitated Risk Analysis and Assessment Process

Thomas R. Peltier

Contents

Introduction

After being in the information security profession for more than 35 years and in information technology for nearly 50 years, I have found that most organizations have the ability to identify threats that can affect the business objectives or mission of the organization. What they cannot do in a systematic manner is to take that threat and determine the level of risk it poses to the organization.

Years ago, I worked with a delightful gentleman named Irving Ball. Irv was six feet seven inches tall and I was five feet two. One morning, Irv came in with a fresh abrasion on his forehead. I inquired as to what happened and Irv asked "Didn't you see that scaffolding in the parking lot?" I said that I thought that I had. At lunch, as we headed to my car, we passed the scaffolding and we noted that the threat to both of us was there. However, the probability of me hitting the portion of the scaffold where Irv did was much lower than for him. So, for both of us, the scaffold was a *threat*. The *risk* to me was lower because the probability and impact were lower.

Just because there is a threat does not mean that the organization is at risk. This is what risk assessment is all about. Identifying the threats that are out there and then determining if those threats pose a real risk to the organization.

With the changing business culture, successful security professionals have had to modify the process of responding to new threats in the high profile, ultra-connected business environment. With outside regulatory agencies and external auditors gaining more oversight strength over the past 5 years, organizations are met with an increased motivation to implement an effective, inexpensive risk assessment process.

Even with the change of focus, today's organizations must still protect the integrity, confidentiality, and availability of information resources they rely on. Although there is an increased interest in security by senior management, the fact remains that the business of the enterprise is business. An effective security program must assist the business units by providing high-quality reliable service in helping them protect the enterprise's assets.

Update

The Facilitated Risk Analysis and Assessment Process (FRAAP) has gone through many changes since it was first used in 1995. This chapter discusses the formal facilitated version of the process. Included in Appendix A is a sample procedure that discusses the latest version. The sample procedure is an example of how a risk assessment process could be deployed at your location. For more on FRAAP, see *Information Security Risk Analysis*, Third Edition.

FRAAP Overview

The FRAAP was developed as an efficient and disciplined process for ensuring that threats to business operations are identified, examined, and documented. The process involves analyzing one system, application, platform, business process, or segment of business operation at a time. By convening a team of internal subject matter experts, the FRAAP will rely on the organization's own people to complete the risk assessment process. These experts must include the business managers and system users who are familiar with the mission needs of the asset under review, and the infrastructure staff who have a detailed understanding of potential system vulnerabilities and related controls. The FRAAP sessions follow a standard agenda and are facilitated by a member of the project office or information security staff. The facilitators are responsible for ensuring that the team members communicate effectively and adhere to the project scope statement. A sample FRAAP procedure has been included Appendix A.

The team's conclusions as to what threats exist, what their risk levels are, and what controls are needed are documented for the business owner's use in developing the FRAAP, and is divided into three phases:

- The pre-FRAAP
- The FRAAP session
- The post-FRAAP

During the FRAAP session, the team will brainstorm to identify potential threats that could affect the task mission of the asset under review. The team will then establish a risk level for each threat based on the probability that the threat might occur and the relative effect were it to occur. We will go into more detail on this process later in the book.

The team does not usually attempt to obtain or develop specific numbers for threat likelihood or annual loss estimates unless the data for determining such factors is readily available. Instead, the team will rely on their general knowledge of threats and probabilities obtained from national incident response centers, professional associations and literature, and their own experience.

When assembling the team, it is experience that allows them to believe that additional efforts to develop precisely quantified risks are not cost-effective because

- Such estimates take an inordinate amount of time and effort to identify and verify or develop
- The risk documentation becomes too voluminous to be of practical use
- Specific loss estimates are generally not needed to determine if a control is needed

After identifying the threats and establishing the relative risk level for each threat, the team identifies controls that could be implemented to reduce the risk, focusing on the most cost-effective controls. The team will use a common set controls designed to address various types of threats. We will discuss the controls selection process later in this chapter.

Once the FRAAP session is complete, the security professional can assist the business owner in determining which controls are cost-effective and meet their business needs. Once each threat has been assigned a control measure or has been accepted as a risk of doing business, then the senior business manager and technical expert participating sign the completed document. The document and all associated reports are owned by the business unit sponsor and are retained for a period to be determined by the records management procedures (usually 7 years).

Each risk assessment process is divided into three distinct sessions:

- The pre-FRAAP meeting, which normally takes about an hour and has the business owner, project lead, scribe and facilitator, and has seven deliverables.
- The FRAAP session takes approximately 4 hours and includes 15 to 30 people, although sessions with as many as 50 and as few as 4 people have occurred.
- Post-FRAAP is where the results are analyzed and the Management Summary Report is completed. This process can take up to five workdays to complete.

During the rest of this chapter, we will examine why the FRAAP was developed and what each one of the three phases entail and what the deliverables are from each phase.

FRAAP History

Before the development of the FRAAP, risk assessment was often perceived as a major task that required the enterprise to hire an outside consultant and could take weeks, if not months, to complete. Often, the risk assessment process was shrouded in mystery and often seemed that elements of voodoo were being used. The final report sometimes looked like the name of your organization was simply edited into a standard report template.

By hiring outside consultants, the expertise of the in-house staff was often overlooked and the results produced were not acceptable to the business unit manager. Additionally, the results of the old process in which business managers were not part of the risk assessment process found that they did not understand the recommended controls, did not want the recommended controls, and often worked to undermine the control implementation process.

What was needed was a risk assessment process that

- Is driven by the business owners
- Takes days instead of weeks or months
- Is cost-effective
- Uses in-house experts

The FRAAP meets all of these requirements and adds another; it can be conducted by someone with limited knowledge of a particular system or business process, but with good facilitation skills.

The FRAAP is a formal methodology developed through understanding the previously developed qualitative risk assessment processes and modifying them to meet the current requirements. It is driven by the business side of the enterprise and ensures that the controls selected enable the business owners to meet their mission objectives. With the FRAAP, controls are never implemented to meet audit or security requirements. The only controls selected focus on the businesses' needs.

The FRAAP was created with an understanding that internal resources had limited time to spend on such tasks. By holding the information-gathering session to 4 hours, then the subject matter experts (SME) are more likely to participate in the process. Using time as a critical factor, the FRAAP addresses as many risk assessment issues as possible. If there is more time, then there are more tasks that can be performed.

By involving the business units, the FRAAP uses them to identify threats. Once the resource owner is involved in identifying threats and then determine the risk level, they generally see the business reason behind why implementing cost-effective controls to help limit exposure is necessary. The FRAAP allows the business units to take control of their resources. It allows them to determine what safeguards are needed and who will be responsible for implementing those safeguards.

The results of the FRAAP are a comprehensive set of documents that will identify threats, prioritize those threats into risk levels, and identify possible controls that will help mitigate those high-level risks.

The FRAAP provides the enterprise with a cost-effective action plan that meets the business needs to protect enterprise resources while ensuring that business objectives and mission charters are met. Most importantly, with the involvement of the business managers, the FRAAP provides a supportive client or owner that believes in the action plan.

Introduce the FRAAP

As with any new process, it is always best to conduct user awareness sessions to acquaint employees before the process is rolled out. It will be necessary to explain what the FRAAP is, how it works, and how it will help the business people meet their specific objectives.

To be successful, the awareness program should take into account the needs and current levels of training and understanding of the employees and management. There are five keys to establishing an effective awareness program. These include

- Assess current level of risk assessment understanding
- Determine what the managers and employees want to learn
- Examine the level of receptiveness to the security program
- Map out how to gain acceptance
- Identify possible allies

To assess the current level of risk assessment understanding, it will be necessary to ask questions of the audience. Although some employees may have been part of a risk assessment in the past, most employees have little first-hand knowledge of risk assessment. Ask questions such as why they believe there is a need for risk assessment. Listen to what the employees are saying and scale the training sessions to meet their specific needs. In the awareness field, one size or plan does not fit for everyone.

Work with the managers and supervisors to understand what their needs are and how the risk assessment process can help them. It will become necessary for you to understand the language of the business units and to interpret their needs. Once you have an understanding, then you will be able to modify the presentation to meet these special needs. No single awareness program will work for every business unit. There must be alterations and a willingness to accept suggestions from non–security personnel.

Identify the level of receptiveness to the risk assessment process. Find out what is accepted and what is meeting with resistance. Examine the areas of noncompliance and try to find ways to alter the program if at all possible. Do not change fundamental risk assessment precepts just to gain unanimous acceptance—this is an unattainable goal. Make the process meet the greater good of the enterprise and then work with pockets of resistance to lessen the impact.

The best way to gain acceptance is to make employees and managers partners in this process. Never decree a new control or policy to the employee population without involving them in the decision-making process. This will require you to do your homework and to understand the business process in each department. It will be important to know the peak periods of activity in the department and what the manager's concerns are. When meeting with the managers, be sure to listen to their concerns and be prepared to ask for their suggestions on how to improve the program. Remember, the key here is to partner with your audience.

Finally, look for possible allies. Find out which managers support the objectives of the risk assessment process and those that have the respect of their peers. This means that it will be necessary to expand the area of support beyond risk management and the audit staff. Seek out business managers that have a vested interest in seeing this program succeed. Use their support to springboard the program to acceptance.

A key point in this entire process is to never refer to the risk assessment process or the awareness campaign as “my program.” The enterprise has identified the need for risk assessment and you and your group are acting as the catalysts to moving the process forward. When discussing the process with employees and managers, it will be beneficial to refer to it as their risk assessment process or our process. Make them feel that they are key stakeholders in this process.

Involve the user community and accept their comments whenever possible. Make the risk assessment process “their” process. Use what they identify as important in the awareness program. By having them involved, then the risk assessment process truly becomes theirs and they are more willing to accept and internalize the results.

Key Concepts

The FRAAP is a formal methodology for risk assessment that is driven by the owner. The asset owner schedules each FRAAP session and the team members are invited by the owner. The concept of what constitutes an owner is normally established in the organization’s information security policy. The policy generally addresses the concepts of information asset owner, custodian, and user. A typical company policy may resemble the following:

- Information created while employed by the company is a company asset and is the property of the company. All employees are responsible for protecting company information from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. To facilitate the protection of company information, employee responsibilities have been established at three levels: *owner*, *custodian,* and *user*.
  - *Owner*: Is the highest level of company management of the organizational unit where the information resource is created, or management of the organizational unit that is the primary user of the information resource. Owners have the responsibility to
    - Establish the classification level of all corporate information within their organizational unit
    - Identify reasonable and prudent safeguards to ensure the confidentiality, integrity, and availability of the information resource
    - Monitor safeguards to ensure that they are properly implemented
    - Authorize access to those who have a business need for the information and
    - Delete access for those who no longer have a business need for the information

- *Custodian*: Employees designated by the owner to be responsible for maintaining the safeguards established by the owner.
- *User*: Employees authorized by the owner to access information and use the safeguards established by the owner.

Senior management must ensure that the enterprise has the capabilities needed to accomplish its mission or business objectives. As we will see, senior management of a department, business unit, group, or other such entity is considered to be the *functional owner* of the enterprise's assets and, in their fiduciary duty, act in the best interest of the enterprise to implement reasonable and prudent safeguards and controls. Risk management is the tool that will assist them in this task (Figure 4.1).

As you can see, the risk assessment process assists management in meeting its obligations to protect the assets of the organization. By being an active partner in the risk assessment process, management, when acting in the owner's capacity, gets the opportunity to see what threats are lurking around the business process. Therefore, FRAAP allows the owner to identify where control weaknesses are and to develop an action plan to remedy the risks in a cost-effective manner.

The results of the FRAAP are a comprehensive risk assessment document that has the threats, risk levels, and controls documented. It also includes an action plan created by the owner with action items, responsible entities identified, and a time frame for completion established. The FRAAP assists management in meeting its obligation to perform due diligence.

A trained facilitator conducts the FRAAP session. This individual will lead the team through the identification of threats, the establishment of a risk level by determining probability and impact, and then the selection of possible safeguards or controls. Because of qualitative risk assessment's subjective nature, it will be the responsibility of the facilitator to lead the team into different areas of concern to ensure that as many threats as possible are identified (Figure 4.2).

Instead of concentrating on establishing audit or security requirements, the facilitator ensures that the risk assessment process examines threats that might affect the business process or the mission of the enterprise. This ensures that only

Typical Role	Risk Management Responsibility
Management Owner	Under the Standard of Due Care, senior management is charged with the ultimate responsibility for meeting business objectives or mission requirements. Senior management must ensure that necessary resources are effectively applied to develop the capabilities to meet the mission requirements. They must incorporate the results of the risk assessment process into the decision-making process.

Figure 4.1 Management owner definition.

Typical Role	Risk Management Responsibility
FRAAP Facilitator	A *facilitator* is someone who skillfully helps a group of people understand their common objectives and assists them in planning to achieve them without taking a particular position in the discussion. The facilitator will try to assist the group in achieving a consensus on any disagreements that preexist or emerge in the FRAAP so that an action plan can be created.

Figure 4.2 FRAAP facilitator definition.

Typical Role	Risk Management Responsibility
FRAAP Scribe	The *scribe* is the individual responsible for taking the oral discussions and creating a written format. The scribe ensures that the threats are properly recorded and all actions of the risk assessment team are captured accurately.

Figure 4.3 FRAAP scribe definition.

those controls and countermeasures that are truly needed and cost-effective are selected and implemented.

Helping the trained facilitator is an individual acting as a recording secretary who will transcribe the meeting and help create the risk assessment documentation. As a scribe, this individual will accurately record the identification of threats and all other relevant information. Unlike an editor, the scribe does not alter the written word once the team has agreed that the meaning of the statement has been properly captured (Figure 4.3).

The Pre-FRAAP Meeting

The pre-FRAAP meeting is the key to the success of the project. The meeting is normally scheduled for an hour and a half and is usually conducted at the business owner's office. The meeting should have the business owner (or representative), the project development lead, facilitator, and the scribe. There will be seven deliverables to come out of this session.

1. *Prescreening results*. The prescreening process is conducted earlier in the System Development Life Cycle (SDLC). Because the risk assessment is a historical record of the decision-making process, a copy of the prescreening results should be entered into the official record and stored in the risk assessment action plan. The prescreening process is discussed in Chapter 3.
2. *Scope statement*. The project lead and business owner will have to create a statement of opportunity for the risk assessment. They are to develop (in

words) what exactly is going to be reviewed. During the pre-FRAAP meeting, the Risk Assessment Scope Statement should be reviewed and edited into the final language.

It is during the development of the scope statement the threat categories need to be determined. In a typical information security risk assessment, we would include the CIA triad of *confidentiality*, *integrity*, and *availability*.

3. *Visual diagram*. There will need to be a visual model. This is a one-page or foil diagram depicting the process to be reviewed. The visual model will be used during the FRAAP session to acquaint the team with where the process begins and ends.

   There is a good reason to require a visual diagram or an information flow model be included as part of the FRAAP. Neural-linguistic programming is a study of how people learn. This process has identified three basic ways in which people learn. These are

   a. *Auditory*—these people have to hear something to grasp it. During the FRAAP, the owner will present the project scope statement to the team and those that learn in this manner will be fulfilled.
   b. *Mechanical*—this learning type must write down the element to be learned. Those taking notes during meetings are typically mechanical learners.
   c. *Visual*—this type of learner, of which most of us are, needs to see a picture or diagram to understand what is being discussed. People who learn through this method normally have whiteboards in their office and use them often. So the visual diagram or model will help these people understand what is being reviewed.

4. *Establish the FRAAP team*. A typical FRAAP has between 15 and 30 members. The team is made up of representatives from a number of business and infrastructure and business support areas.
5. *Meeting mechanics*. This is the business unit manager's meeting and he or she is responsible for scheduling the room, setting the risk assessment time, and having the appropriate materials (overhead, flip charts, coffee and doughnuts) on hand.

   This risk assessment meeting is the responsibility of the owner. As the facilitator, you are assisting the owner in completing this task. It is not an information security, project management office, audit, or risk management meeting. It is the owner's meeting and that person is responsible for scheduling the place and inviting the team.
6. *Agreement on definitions*. The pre-FRAAP session is where the agreement on FRAAP definitions is completed. These definitions will eventually become a standard used in the risk assessment process. However, it is always a good idea to review the concepts that will be used in the risk assessment (Figure 4.4).

Term	Definition
Asset	A resource of value. An asset may be a person, physical object, process, or technology
Threat	The potential for an event, malicious or otherwise, that would damage or compromise an asset
Probability	A measure of how likely a threat may occur
Impact	The effect of a threat being carried out on an asset—expressed in tangible or intangible terms
Vulnerability	Any flaw or weakness in the asset's defenses that could be exploited by a threat to create an impact on the asset
Risk	The combination of threat, probability, and impact expressed as a value in a predefined range

Figure 4.4 Risk assessment definitions.

You will want to agree on the definitions of the business attributes to be used as these will become your review elements. For many risk assessments, we have examined integrity, confidentiality, and availability. Recently, a group of my fellow information security professionals and I examined the idea of which attributes should be examined. For years, we concentrated on examining the threats associated with the security triad on confidentiality, integrity, and availability (CIA).

Although CIA is a traditional form of risk assessment, it is important to understand that there are other business attributes that can be used in the process. When I was in college, in our Psychology 101 class and we discussed *functional fixedness*, which is a cognitive bias that limits a person to using an object only in the way it is traditionally used. When you give a child a present, they oftentimes have more fun playing with the wrappings or the box. That is because the wrappings can be anything.

I use this example in my training classes to remind audit, information security, and risk management that there are a vast number of business attributes that can be used to determine risk. Even if your primary use of risk assessment is to determine threats to assets based on examining confidentiality, integrity, and availability—try to remain open to other possibilities.

I sent a question out to my colleagues and posed the following question:

> "When we are conducting risk assessments, we often examine threats based on CIA. We also discussed earlier this week that instead of CIA, we could consider reliability-performance-cost (for capital) or

> portability-scalability-market penetration (for software) as examples. Does the use of these categories divide our way of thinking? Could this be titled *threat categories*? Also, do we do it this way because it is required or because it helps us think better within set boundaries?"
>
> CIA, reliability-performance-cost, and portability-scalability-market penetration are just nine of the hundreds of such things defined in the Sherwood Applied Business Security Architecture (SABSA) method since 1996. We call them "business attributes" and the business attributes profile is used as the basis for all risk management.
>
> The default prompt list/modeling tool kit has the 80 attributes that are most often reused internationally (see www.sabsa.org), although each organization has a different context and thus a different set.
>
> We have a whole section dedicated to users' definitions of these things and demonstrating case studies on the Institute web site. Sadly, that part of the site (it is in the member discussion area) isn't publicly accessible yet, but we've about 200 people impatiently waiting on it out of the hundreds that are now certified in the method.
>
> *Could this be titled Threat Categories?*
>
> I don't believe so. They are not threats but the areas/things of value we want to protect from the threats, that is, ultimately, the business things that are at risk. Thus, the use of the term business attributes seems to fit best.
>
> However, they can easily be used to create a threat modeling taxonomy and they often are used that way in daily practice. Also, although you have correctly seen potential demarcation lines between different types (you used capital and software), a whole enterprise-wide taxonomy can be constructed that defines the things of value both unique to a division/stakeholder/department/team/project and to the enterprise as a whole. That in turn provides the basis for risk aggregation.
>
> *Also, do we do it this way because it is required or because it helps us think better within set boundaries?*
>
> I believe that it is the latter. It isn't actually required but it helps. Boundaries and structure of many kinds help remove the horrendous subjectivity and variable response we would get from a blank unbounded or unstructured risk management canvas.

The business attributes that are going to be used in the risk assessment process must be discussed and agreed upon. A formal set of definitions must also be established. The following are examples of some of the many business attributes that can be used to examined threats and establish risk levels (Figures 4.5 through 4.7).

CIA Example	
Term	**Definition**
Availability	Assuring information and communications services will be ready for use when expected
Confidentiality	The assurance that information is not disclosed to inappropriate entities or processes
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed

Figure 4.5 Business attribute definitions (CIA).

Capital Expenditure Example	
Term	**Definition**
Reliability	The extent to which the same result is achieved when a measure is repeatedly applied to the same asset
Performance	A quantitative measure characterizing a physical or functional attribute relating to the execution of a mission/operation or function
Cost	The total spent for goods or services including money, time, and labor

Figure 4.6 Business attribute definitions (capital expenditure).

Software Procurement Example	
Term	**Definition**
Portability	A measure of system independence; portable programs can be moved to a new system by recompiling without having to make any other changes
Scalability	The ability to expand a computing solution to support large numbers of users without affecting performance
Market Penetration	The share of a given market that is provided by a particular good or service at a given time

Figure 4.7 Business attribute definitions (software procurement).

During the pre-FRAAP session, it will be important to discuss the process for prioritizing threats. When examining the probability and impact of threats, it will be necessary to determine before the meeting if the threats are to be examined as if no controls are in place. This is typically the case when doing a risk assessment on an infrastructure resource. These resources include the information processing network, the operating system platform, and even the information security program.

For other applications, systems, and business processes, the examination of threats takes into account existing controls. When we discuss the FRAAP session, we will examine each of these methods and how they work. This decision should be made during the pre-FRAAP meeting. Once the risk assessment process has been established, this discussion will not be necessary because the organization will standardize the risk level protocol.

Pre-FRAAP Meeting Checklist

When I attend a pre-FRAAP meeting, I like to take with me a checklist that will ensure that I receive all of the items I need to complete the pre-FRAAP process (Figure 4.8).

Issue	**Remarks**
Before the Meeting	
1. Date of Pre-FRAAP Meeting *Record when and where the meeting is scheduled*	
2. Project Executive Sponsor or Owner *Identify the owner or sponsor who has executive responsibility for the project*	
3. Project Leader *Identify the individual who is the primary point of contact for the project or asset under review*	
4. Pre-FRAAP Meeting Objective *Identify what you hope to gain from the meeting—typically the seven deliverables will be discussed*	
5. Project Overview *Prepare a project overview for presentation to the pre-FRAAP members during the meeting*	
Your understanding of the project scope	
The FRAAP methodology	
Milestones	
Prescreening methodology	
6. Assumptions *Identify assumptions used in developing the approach to performing the FRAAP project*	

Figure 4.8 Pre-FRAAP meeting checklist.

7. Prescreening Results *Record the results of the prescreening process*	
During the Meeting	
8. Business Strategy, Goals, and Objectives *Identify what the owner's objectives are and how they relate to larger company objectives*	
9. Project Scope *Define specifically the scope of the project and document it during the meeting so that all participating will know and agree*	
• Applications/Systems	
• Business Processes	
• Business Functions	
• People and Organizations	
• Locations/Facilities	
10. Time Dependencies *Identify time limitations and considerations the client may have*	
11. Risks/Constraints *Identify risks and/or constraints that could affect the successful conclusion of the project*	
12. Budget *Identify any open budget/funding issues*	
13. FRAAP Participants *Identify by name and position the individuals whose participation in the FRAAP session is required*	
14. Administrative Requirements *Identify facility and/or equipment needs to perform the FRAAP session*	
15. Documentation *Identify what documentation is required to prepare for the FRAAP session (provide the client the FRAAP Document Checklist)*	

Figure 4.8 (Continued) Pre-FRAAP meeting checklist.

Figure 4.9 gives direction on filling out the pre-FRAAP meeting checklist.

By completing this checklist, the elements for the project scope statement will be nearly complete. Two of the key elements contained in the checklist, and that must be part of the project scope statement, are the categories of *assumptions* and *constraints*. It is important that we understand what these are and how they affect the risk assessment process.

Issue	Activity
Before the Meeting	
1. Date of Pre-FRAAP Meeting	Record the date the actual pre-FRAAP meeting occurred
2. Project Executive Sponsor or Owner	Record the full name and proper title of the owner of the asset that is to be reviewed
3. Project Leader	Record the full name and proper title of the project lead for this specific asset or task
4. Pre-FRAAP Meeting Objective	There are seven deliverables for the pre-FRAAP meeting: • Scope statement • Visual model • Assessment Team • Definitions • Meeting Mechanics • Prescreening results • Mini Brainstorming Results
5. Project Overview	If the FRAAP is a new concept to the owner and/or project lead, provide them with an overview of the process
Your understanding of the project scope	
The FRAAP methodology	
Milestones	
Prescreening methodology	
6. Assumptions	Record any issues that are needed to support the project scope statement
7. Prescreening Results	Record the prescreening results

Figure 4.9 Pre-FRAAP meeting checklist directions.

During the Meeting	
8. Business Strategy, Goals, and Objectives	Record the mission of the asset under review and how it supports the overall business objectives or mission of the enterprise
9. Project Scope	Draft the FRAAP scope statement
• Applications/Systems	
• Business Processes	
• Business Functions	
• People and Organizations	
• Locations/Facilities	
10. Time Dependencies	Identify any time issues and enter them into the constraints section of the scope statement
11. Risks/Constraints	Record any issues that may affect the results of the FRAAP
12. Budget	Where appropriate, establish a work order number of project identification number that FRAAP team members can use to report time spent on specific projects.
13. FRAAP Participants	Record who the stakeholders are and other team members as requested by the owner
14. Administrative Requirements	Record any special requirements needed for the FRAAP session
15. Documentation	Record all laws, regulations, standards, directives, policies, and/or procedures that are part of the infrastructure supporting the asset under review

Figure 4.9 (Continued) Pre-FRAAP meeting checklist directions.

I have a client who brings me in from time to time to conduct FRAAP refresher training for employees. It gives the employees who have previously taken the training a chance to be exposed to new ideas and concepts, and for other employees to be exposed to the process for the first time. Typically, this process is done over 3 or 4 days. It consists of a day and a half of training and then in the afternoon of day two, the pre-FRAAP meeting is conducted. The following day, the FRAAP session is conducted and then, that afternoon and the following day, I work with the project leader and the facilitator to complete the risk assessment documentation.

On the afternoon of day one, the project leader and his backup informed me that they had a meeting to attend and would be back the following day. Not only did they miss the afternoon training of day one, they also did not return for any of the day two training. On the afternoon of day two, the attendees that were there decided to try and put together a project scope statement. The audience was almost exclusively information security and audit professionals. The scope statement lacked the business side, but at least we were able to be ready for the following day. Because of the team makeup, we did not address assumptions or constraints.

On the day of the FRAAP session, the project leaders returned with the owner. This was the first time the owner had ever been exposed to a risk assessment process. We presented them with the scope statement that we had created and the owner said that it looked okay to her. So, after a brief introduction and an overview of the methodology, we began the process of identifying threats. After approximately 2 hours, the team had identified nearly 150 threats. As we were working through the FRAAP session, I noticed that owner's face had initially turned red and at the break was now white. I approached her to see if there was a problem. She informed me that the system was going into production on the following Monday and there was no way she could tell her bosses that 150 threats were uncovered.

During the break, I thought about what had transpired and when she came back I sat down with her to review the scope statement and to fill in the assumption area. A number of the threats identified were directly related to elements within the information security program. Threats such as

- Passwords being posted on workstations
- Employees leaving workstations logged on and unattended
- Employees leaving work materials out after hours
- Shoulder surfing passwords or other access codes
- Unauthorized access to restricted areas

Although these were important threats, they were already addressed in the risk assessment conducted on the information security infrastructure previously and were not unique to the specific application under review. By modifying the assumption section of the scope statement to include a reference to the fact that it was assumed that a risk assessment had been conducted on the information security infrastructure and that compensating controls were in place or were being implemented. We also addressed the processing infrastructure and applications development methodology in the same manner. By making sure the assumptions were properly identified, we reduced the number of threats from approximately 150 to approximately 30.

The FRAAP was not diminished in any way. The 120 or so threats that were exercised from the risk assessment report had already been identified in the infrastructure risk assessments and were being acted on. If other risk assessments have been conducted, then enter that information into the assumptions area.

If the infrastructure risk assessments have not been conducted, then enter that information into the constraints area. This will allow the risk assessment to concentrate on the specific asset at hand, but puts the organization on notice that other risk assessments must be scheduled.

Integrity	Confidentiality	Availability
Data stream could be intercepted	Insecure e-mail could contain confidential information	Files stored in personal directories may not be available to other employees when needed
Faulty programming could (inadvertently) modify data	Internal theft of information	Hardware failures could affect the availability of company resources
Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons	Employee is not able to verify the identity of a client, example: phone masquerading	A failure in the data circuit could prohibit system access
Data could be entered incorrectly	Confidential information is left in plain view on a desk	Act of God—tsunami/ hurricane
Intentional incorrect data entry	Social discussions outside the office could result in disclosure of sensitive information	Upgrades in the software may prohibit access

Figure 4.10 Mini brainstorming results.

Other constraints might include the concerns about the use of obsolete operating system, those that are no longer supported by the manufacturer. The back level of the patch application might also be a constraint to identify.

Assumptions and constraints allow the risk assessment team to focus on the asset at hand. The organization must conduct the other risk assessments to make certain that the infrastructure is as secure as possible.

Over the past 2 years, an extra process has been added to the pre-FRAAP portion of the risk assessment process. That extra element is a brief mini brainstorming process. At the end of the pre-FRAAP session, those assembled should conduct a quick threat identification process. Using each of the business attributes that are to be examined, the pre-FRAAP team will identify threats to the asset just as the entire team will during the FRAAP session. It will be important to get four or five threats for each business attribute. The FRAAP facilitator will use this information during the FRAAP session (Figure 4.10).

Pre-FRAAP Meeting Summary

The pre-FRAAP meeting sets the stage for the FRAAP session and all of the work that is to follow. It is very important that each of the seven deliverables be as complete as possible. If they are not complete, then this could be a major constraint to the risk assessment process.

The FRAAP Session

Overview

The FRAAP session is typically scheduled for 4 hours. This is a very tight timeframe and can be expanded if you have the time and resources available. During the past 2 years, I have been back out in the field conducting FRAAPs for various clients. The 4-hour window is sufficient to capture threats associated with the business attributes of a specific asset. Then identify existing controls and conduct a risk level analysis of the threats to identify those risks that require risk remediation. As we discussed earlier, the key component in the development of the FRAAP was the time commitment that was available from the team members.

Think about the typical employee schedule at work each week. How much free or available time do you have each week? For many of us, we donate at least 12 hours of our workweek to meetings. For the people that will be asked to participate in the risk assessment process, there will be an effect on their available time. The FRAAP is designed to meet the needs of an effective risk assessment while affecting the team members as little as possible.

FRAAP Session Introduction

Once the FRAAP session is called together, the executive responsible for the asset under review will address the team with opening remarks. This overview will help the team understand why they were asked to be part of the FRAAP and how important senior management considers the risk assessment process to be. When the overview is complete, the facilitator will present the agenda to the team. A typical agenda might include the items listed in Figure 4.11.

FRAAP Session Agenda	Responsibility
• Explain the FRAAP process	Facilitator
• Review scope statement	Owner
• Review visual diagram	Technical support
• Discuss definitions	Facilitator
• Review objectives • Identify threats • Establish risk levels • Identify possible safeguards	Facilitator
• Identify roles and introduction	Team
• Review session agreements	Facilitator

Figure 4.11 FRAAP session agenda.

The facilitator will explain the FRAAP to the team. This will include a discussion on the deliverables expected from each stage of the process. With the assistance of the facilitator, the team will identify threats to the asset under review. Using a formula of probability and impact, the team will then affix a risk level to each threat and, finally, the team will select possible controls to reduce the risk intensity to an acceptable level.

The business manager/owner will then present the project scope statement. It will be important to discuss the assumptions and constraints identified in the statement. The team should have a copy of the scope statement that they can refer to as the need arises during the FRAAP session. The assumptions and constraints will be helpful in ensuring that the deliverables are as accurate as possible.

The technical support will then give a 5-minute overview of the process using an information flow model or diagram. This will allow the team to visualize the process under review.

The facilitator will then review the term definitions to be used for this FRAAP session. Once the risk assessment process becomes part of the organization's culture, these definitions will become standard and the need for review will diminish. To expedite the process, the FRAAP session definitions should be included in the meeting notice.

The facilitator will then reiterate the objectives and deliverables of this initial stage. At this point, stage two of this process should be briefly discussed. In the meeting notice, it will be necessary to notify those individuals that are needed to be present for stage two that they will be staying for an additional hour.

At this point, the FRAAP team should introduce itself. Have each member introduce themselves and provide the following information for the scribe to capture:

- Team member name (first and last)
- Department
- Location
- Phone number

After the introductions, the facilitator will review the session agreements with the team members (Figure 4.12).

FRAAP Session Talking Points

Everyone participates—it is important to get input from everyone in attendance. There will be those that will want to sit back for the first few minutes to get the lay of the process and become comfortable. Some of this apprehension can be alleviated by having a FRAAP awareness session throughout your organization. Many times, it is the fear of the unknown that causes team

Session Agreements
• Everyone participates
• Stay within identified roles
• Stick to the agenda/current focus
• All ideas have equal value
• Listen to other points of view
• No “plops”... all issues are recorded
• Deferred issues will be recorded
• Post the idea before discussing it
• Help scribe ensure all issues are recorded
• One conversation at a time
• One angry person at a time

Figure 4.12 FRAAP session agreements.

members to hold back. By conducting brief awareness sessions that explain the reasons for and the process done by the risk assessment process, the team members will have a greater feeling of participation.

Stay within identified roles—introduce the facilitator and scribe. Explain that your job is to get the FRAAP completed within the limited timeframe. The scribe will record all of the agreed upon findings of the risk assessment. All others present are team members. As they enter the room, they initially take off current roles and put on the team member role.

Stick to the agenda/current focus—the reason that the scope statement and visual model are discussed early in the process is so that every one is reminded of what the focus of the FRAAP meeting is. We all have attended meetings in which the intended purpose seems to get thrown out and anything else possible is discussed. It will be your job to keep the team on focus.

All ideas have equal value—this one is very difficult. As discussed above, some people are a bit intimidated by other team members. Sometimes, the users are apprehensive to discuss threats to applications or system while IT infrastructure personnel are present. It will be necessary for everyone to feel that their ideas are just as important as anyone else’s.

Listen to other points of view—many times in meetings, some attendees break out of the group and carry on private conversations. At the beginning of the session, we try to remind the team that the best way we can show the respect we want is by showing respect to others.

No "plops"—all issues are recorded—at least once in every session, someone will comment that "This may seem stupid, but…" and then they present a unique twist to the issues being discussed. One of the many questions that arise when a risk assessment decision is being questioned is "What did you consider?" This very question is why it is important to record all issues.

Deferred issues will be recorded—in the FRAAP documentation, there is a spot to record any issue that is outside the scope of the current meeting. This will allow the team to record the concern and assign someone to follow up on it.

Post the idea before discussing it—there will be a period of discussion on what the threat is and then there will often be some editing and finally the scribe will post the agreed upon item.

Help the scribe ensure that all issues are recorded—although there are time constraints on completing the session, it is vitally important to capture the issues and comments correctly.

One conversation at a time—as we discussed above, it is important for the team to keep focused on the task at hand. If a number of separate conversations break out, then the objectives of the FRAAP session may not be completed during the allotted time.

Apply the 3- to 5-minute rule—when discussing the risk level setting factors, it is important that after the first three or four discussions that a time limit be more or less adhered to.

When all of the preliminary activities have been concluded, it is time to begin the risk assessment process.

FRAAP Threat Identification

When I conduct a FRAAP, I like to have the room set up in a "U" shape. This allows me to work closer to the team members and it allows the process to flow around a conference room table. By being set up in this manner, everyone is in the front row. If the room is set up classroom style it is harder to get the people in the back to feel that they are part of the team.

In the room setup, it is important to include pads of paper and pens or pencils for the team to use. The team will be writing down their ideas and it is always best to have the implements readily available than to take time to try and find them.

During the FRAAP session, I normally discourage the use of laptops or PDAs. The team has been called by the owner to assist them in meeting their due diligence obligation. If the team members are busy answering e-mails or distracted by other activities, the risk assessment will suffer. I also request that all cell phones and pagers be placed on "stun" or vibrate so as not to disturb the other team members.

To begin the brainstorming process, the facilitator will put the first business attribute to be reviewed up for the team to see. This will include the definition of the review element and some examples of threats that the team can use as thought starters. I normally use a PowerPoint slide for this process so that the entire team can see what it is that the FRAAP is trying to identify (Figure 4.13).

The team is given 3 to 5 minutes to write down threats that are of concern to them. The facilitator will then go around the room getting one threat from each team member. Many will have more than one threat, but the process is to get one threat and then move to the next person. This way everyone gets a turn at participating. The process continues until everyone passes (that is, there are no more threats that the team can think of).

During the first two rounds, most of the team members will participate. As the rounds progress, the number of team members with new threats will diminish. When it gets down to just a few still responding, you can just ask for a new threat from anyone rather than going around the table and calling on each person again.

If a person passes, it does not mean that they are then locked out of the round. If something new comes into their mind, then they can join back in when it is their turn to do so again. They may hear a threat from someone else that will jog their thought process. This is why I recommend that there be paper and pens available for the team members to write down these quick-hitting ideas. Most all of us suffer from terminal CRS (can't remember stuff). By providing paper and pens, the team members can capture these fleeting thoughts.

I am sad to point out that, to some people, everything is a contest. Too often, the brainstorming round will dwindle down to two team members. When this occurs, the battle to be "King of the Threats" begins. They will continue to throw out ever more absurd threats until one will finally yield. I share this with you only so that you can be on the alert for such behavior.

Integrity	
Definition: assuring information will not be accidentally or maliciously altered or destroyed	Threats
	Data stream could be intercepted
	Faulty programming could (inadvertently) modify data
	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons
	Data could be entered incorrectly
	Intentional incorrect data entry

Figure 4.13 FRAAP brainstorming attribute 1.

Confidentiality	
Definition: the assurance that information is not disclosed to inappropriate entities or processes	Threats
	Insecure e-mail could contain confidential information
	Internal theft of information
	Employee is not able to verify the identity of a client, example: phone masquerading
	Confidential information is left in plain view on a desk
	Social discussions outside the office could result in disclosure of sensitive information

Figure 4.14 FRAAP brainstorming attribute 2.

Once all of the integrity threats have been recorded, it is time for the facilitator to display the second review element with threat examples and give the team 3 to 5 minutes to write down their threats (Figure 4.14).

During this phase, I like to start the threat identification on the opposite side of the room from where I started last time. This allows those who were last to be first and get the best threats. The collecting of threats will continue until everyone has passed and there are no more confidentiality threats. After the scribe has indicated that everything has been captured, it will be time to go to the third element (Figure 4.15).

Availability	
Definition: assuring information and communications services will be ready for use when expected	Threats
	Files stored in personal directories may not be available to other employees when needed
	Hardware failures could affect the availability of company resources
	A failure in the data circuit could prohibit system access
	Act of God—tsunami/hurricane
	Upgrades in the software may prohibit access

Figure 4.15 Brainstorming attribute 3.

Once the threats have been recorded, the FRAAP documentation will look like Figure 4.16.

Business Attribute	Threat		
Integrity	Data stream could be intercepted		
Integrity	Faulty programming could (inadvertently) modify data		
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons		
Integrity	Data could be entered incorrectly		
Integrity	Intentional incorrect data entry		
Confidentiality	Insecure e-mail could contain confidential information		
Confidentiality	Internal theft of information		
Confidentiality	Employee is not able to verify the identity of a client, example: phone masquerading		
Confidentiality	Confidential information is left in plain view on a desk		
Confidentiality	Social discussions outside the office could result in disclosure of sensitive information		
Availability	Files stored in personal directories may not be available to other employees when needed		
Availability	Hardware failures could affect the availability of company resources		
Availability	A failure in the data circuit could prohibit system access		
Availability	Act of God—tornado/hurricane		
Availability	Upgrades in the software may prohibit access		

Figure 4.16 FRAAP worksheet 1 after threats have been identified.

When I am conducting a FRAAP session, I use different color pens for each element. Integrity might be blue, confidentiality green, and availability recorded in black. This will allow me to keep track of the threats by color-coding them. As a flip chart page is filled up, I post it around the conference room. I record each threat sequentially within an element. For example, I will record all integrity threats in blue and number each threat in the order it was received starting with threat one. When I move to confidentiality threats, I will switch to a green marker and start the numbering over again with one. I will do the same when I get to the availability threats.

When all the threats have been posted, I recommend that the team be given a 15-minute coffee break to do three important activities:

- Check messages
- Get rid of old coffee and get new
- Clean up the raw threats

As the team is having its break, have them review the threats and within the specific element delete duplicate threats and combine like threats. If a threat is repeated in the integrity and confidentiality element, it is not considered to be a duplicate. It is only a duplicate if it appears more than once within a specific element. Only allow 15 minutes of the break for the clean-up process.

Identify Threats Using a Checklist

During the past few years, some organizations have faced the task of doing a large number of risk assessments to become compliant with specific new laws and regulations. HIPAA is one specific example. A number of health care organizations contacted me to help them put together their risk assessment program. When we began to examine their specific needs, we found out that they did not have 4 hours for the risk assessment process. They found that they could get people to commit to a 2-hour window. So, from there, we worked to find ways to streamline the process. We were able to meet the 2-hour window by creating a checklist of threats to work off of. The results of this work are available for you in Appendix A: Facilitated Risk Analysis and Assessment Process (FRAAP) (see Figure 4.17).

To keep the risk assessment as clear as possible, we will concentrate on the activities that take place using the brainstorming techniques. When we have completed that discussion, we will turn our attention to the checklist style of risk assessment.

Identifying Existing Controls

Once the threats list has been completed, the team should quickly review each threat and determine if there are any existing controls in place that address those

Threat	Applicable (Yes/No)					
Environmental						
Power flux						
Power outage—internal						
Power outage—external						
Water leak/ plumbing failure						
HVAC failure						

Figure 4.17 Sample threat checklist.

threats issues. By identifying those threats that have existing controls in place, the team will be better able to determine the real current risk level. This is one of the many reasons that the FRAAP needs representation from the various infrastructure groups. They will typically know best what controls and safeguards are already implemented (Figure 4.18).

Business Attribute	Threat	Existing Controls
Integrity	Data stream could be intercepted	Vacant ports are disconnected
Integrity	Faulty programming could (inadvertently) modify data	Programs are tested before going into production, and change management procedures are in place. Gramm Leach Bliley Act's (GLBA's) Information Technology Policies and Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons	
Integrity	Data could be entered incorrectly	Transaction journals are used. Contracts with third parties include language that addresses data integrity and service level agreements are designed to protect against this risk

Figure 4.18 FRAAP worksheet 2 after existing controls have been identified.

Integrity	Intentional incorrect data entry	Transaction logs are maintained and reviewed to detect incorrect data entry
Confidentiality	Insecure e-mail could contain confidential information	
Confidentiality	Internal theft of information	GLBA's Code of Conduct Policy
Confidentiality	Employee is not able to verify the identity of a client, example: phone masquerading	Customer must provide the date of last deposit, or other confidential personal information within their file, and give to the employee before information is released
Confidentiality	Confidential information is left in plain view on a desk	
Confidentiality	Social discussions outside the office could result in disclosure of sensitive information	Code of Conduct/Conflict of Interest Policy. Annual Awareness item
Availability	Files stored in personal directories may not be available to other employees when needed	GLBA's management has established written policies and procedures to ensure information resources are available. See GLBA's Information Technology Policies and Procedures Manual No. 8-1 and Information Technology Policies and Procedures Manual No. 7-4
Availability	Hardware failures could affect the availability of company resources	GLBA's management has established written policies and procedures to ensure information resources are available. See GLBA's IT P&P No. 8-1 and IT P&P No. 7-4 Vendor maintenance agreements are established to support timely resolution of hardware failures. Files are imaged and stored to support recovery of information (ghost files)
Availability	A failure in the data circuit could prohibit system access	Vendor maintenance agreements are established to support timely resolution of hardware failures. See Information Technology Policies and Procedures Manual No. 2-2

Figure 4.18 (Continued) FRAAP worksheet 2 after existing controls have been identified.

Availability	Act of God—tornado/hurricane	
Availability	Upgrades in the software may prohibit access	GLBA's management has established written policies and procedures to ensure that software is tested before use in a production environment. See GLBA's Information Technology Policies & Procedures Manual 3-1 and IT P&P Manual 4-18

Figure 4.18 (Continued) FRAAP worksheet 2 after existing controls have been identified.

Establish Risk Levels

This is probably the most important portion of the FRAAP and often the most confusing and most fun. You will want to ensure that the team has had an opportunity to examine the definitions used to establish probability and impact threshold levels. I like to include this information in the meeting notice attachments. This process will also be discussed during your FRAAP awareness program and briefly reviewed in the FRAAP session opening remarks.

For our initial review of the risk level setting process, we will use a very simple example of the probability and impact thresholds.

At this point in the FRAAP, we have identified threats to the asset under review using the agreed upon business attributes. We then examined each threat and identified those that had existing controls or safeguards in place. Our next task will be to determine how likely that threat will occur the next time and what effect to the organization there would be if the threat were to occur (Figure 4.19).

The team will discuss how likely the threat is to occur during the specified time frame. What you will want to do is to apply a good dose of common sense to the discussion. One of the examples that I like to use is the threat that an unattended workstation could be used by some other person to access the system. A good reality

Term	Definition
Probability	A measure of how likely a threat may occur
Threshold Level	
High	Very likely that the threat will occur within the next year
Medium	Possible that the threat will occur within the next year
Low	Highly unlikely that the threat will occur within the next year

Figure 4.19 FRAAP probability thresholds.

check is what you want to instill in this process. In the 30 years I have been in information security, this threat has always made every discussion list. I am not certain that I can cite one example of this threat actually occurring.

So when you discuss probability, you will want them to address if this threat has actually occurred. If so, when was the last time that the threat did occur? This will provide the team with an ongoing reality check. You will want to keep them focused on the fact that the threats are being examined with existing controls in place.

Once the probability has been established, you will want to identify the impact presented by that threat to the asset under review (Figure 4.20).

Here, again, it will be necessary to work with the team to ensure that the impact level is actually understood. Many times in the FRAAP, the business owner or users will get the impression that if their business unit is affected, then the impact level is rated high. Typically, that is not the case. A high impact level is used to identify those threats that would affect the entire organization. One way to help the team see the issue in the proper light is to ask if the threat has ever occurred. If it has, then we want to discuss what the effect really was.

I recently conducted a risk assessment in which the threat identified was that contractors could enter data incorrectly into the system. Initially, the discussion was that the probability of occurrence was high and that it had the possibility to severely affect the entire mission of the agency. I asked the question about the high probability and found out that this issue happened on an almost daily basis. With that information, we turned our attention to the effect. Although it was true that there was a chance that the entire agency could be affected, the fact that existing controls had prevented it from reaching that level seemed to mean that something less than a high impact was the correct answer.

It helps to work with the team for the first few threats to make certain that everyone sees how the process works. Once the probability and impact have been selected, it will be easy to identify the risk level (Figure 4.21).

Term	Definition
Impact	The effect of a threat being carried out on an asset—expressed in tangible or intangible terms
Threshold Level	
High	Entire mission or business is affected
Medium	Loss limited to single business unit or business objective
Low	Business as usual

Figure 4.20 FRAAP impact thresholds.

	Impact			
		Low	Medium	High
Probability	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Figure 4.21 FRAAP probability/impact matrix.

Color	**Risk Level**	**Action**
Red	High	Requires immediate action
Yellow	Medium	May require action, must continue to monitor
Green	Low	No action required at this time

Figure 4.22 Risk level color key.

The team can examine where the probability and impact levels fall and then can assign a risk level (Figure 4.22).

Therefore, the results would look like Figure 4.23.

Residual Risk

When examining a threat, there are typically two types of risk that will be identified. In the example below, there are three total risks identified. The first two have existing controls in place and the third threat does not. After performing the probability/impact process in the first two threats, the risk level that will be established is termed the *residual risk*. The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no system is risk-free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

For the third threat, because there are no existing controls in place, the risk level established is termed the *baseline risk level*. The baseline risk level (Figure 4.24) is created by establishing the probability and impact of a threat with no control selected. This is done to determine if the risk is great enough to require further action.

After the risk levels have been established, it will be necessary to assess if the risk level is acceptable. There are a number of factors that will ultimately determine if the risk level is acceptable. For the purposes of this exercise, we will state that any risk level of medium or high level must be reexamined to determine if additional controls could lower the risk level (Figure 4.25).

The final process in the FRAAP session is to identify controls for those threats identified as having a high risk level. In the example, those would be anything

Business Attribute	Threat	Existing Controls	Probability/ Impact	Risk Level
Integrity	Data stream could be intercepted	Vacant ports are disconnected	L/M	Low
Integrity	Faulty programming could (inadvertently) modify data	Programs are tested before going into production, and change management procedures are in place. GLBA's Information Technology Policies and Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard	L/L	Low
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons		M/M	Medium
Integrity	Data could be entered incorrectly	Transaction journals are used. Contracts with third parties include language that addresses data integrity and service level agreements are designed to protect against this risk	M/L	Low
Integrity	Intentional incorrect data entry	Transaction logs are maintained and reviewed to detect incorrect data entry	L/M	Low
Confidentiality	Insecure e-mail could contain confidential information		L/H	Medium
Confidentiality	Internal theft of information	GLBA's Code of Conduct Policy	L/L	Low
Confidentiality	Employee is not able to verify the identity of a client, example: phone masquerading	Customer must provide the date of last deposit, or other confidential personal information within their file, and give to the employee before information is released	L/H	Medium
Confidentiality	Confidential information is left in plain view on a desk		M/M	Medium

Figure 4.23 FRAAP worksheet 3 with risk levels assigned.

Business Attribute	Threat	Existing Controls	Probability/ Impact	Risk Level
Confidentiality	Social discussions outside the office could result in disclosure of sensitive information	Code of Conduct/Conflict of Interest Policy. Annual Awareness item	M/M	Medium
Availability	Files stored in personal directories may not be available to other employees when needed	GLBA's management has established written policies and procedures to ensure information resources are available See GLBA's Information Technology Policies and Procedures Manual No. 8-1 and Information Technology Policies and Procedures Manual No. 7-4	L/H	Medium
Availability	Hardware failures could affect the availability of company resources	GLBA's management has established written policies and procedures to ensure information resources are available See GLBA's IT P&P No. 8-1 and IT P&P No. 7-4 Vendor maintenance agreements are established to support timely resolution of hardware failures Files are imaged and stored to support recovery of information (Ghost files)	L/L	Low
Availability	A failure in the data circuit could prohibit system access	Vendor maintenance agreements are established to support timely resolution of hardware failures. See Information Technology Policies and Procedures Manual No. 2-2	L/L	Low
Availability	Act of God—tornado/hurricane		M/H	High
Availability	Upgrades in the software may prohibit access	GLBA's management has established written policies and procedures to ensure that software is tested before use in a production environment See GLBA's Information Technology Policies and Procedures Manual 3-1 and IT P&P Manual 4-18	L/L	Low

Figure 4.23 (Continued) FRAAP worksheet 3 with risk levels assigned.

Business Attribute	Threats	Existing Controls	Probability/ Impact	Risk Level
Integrity	Data stream could be intercepted	Vacant ports are disconnected	L/M	Low
Integrity	Faulty programming could (inadvertently) modify data	Programs are tested before going into production, and change management procedures are in place. GLBA's Information Technology Policies and Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard	L/L	Low
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons		M/M	Medium

Residual Risk

Baseline Risk Level

Figure 4.24 FRAAP residual risk/baseline risk level.

identified as having a risk level of "high" or "medium." A sample control list should be sent out to all team members along with the meeting notice and copies should be available for the team during the FRAAP session.

During this step, the risk assessment team will determine which security controls generally could best reduce the threat risk level to a more acceptable level. There are a number of sources for standards that can assist the risk assessment team in establishing an effective set of controls. These sources might include some of the following:

- Information Technology—Code of Practice for Information Security Management (ISO/IEC 27002)
- Security Technologies for Manufacturing and Control Systems (ISA-TR99.00.01-2004)
- Integrating Electronic Security into Manufacturing and Control Systems Environment (ISA-TR99.00.02-2004)
- Federal Information Processing Standards Publications (FIPS Pubs)
- National Institute of Standards and Technology
- CobiT Security Baseline
- Health Insurance Portability and Accountability Act (HIPAA)
- The Basel Accords
- Privacy Act of 1974

Business Attribute	Threat	Existing Controls	Probability/ Impact	Risk Level	Acceptable Level (Yes/No)
Integrity	Data stream could be intercepted	Vacant ports are disconnected	L/M	Low	Yes
Integrity	Faulty programming could (inadvertently) modify data	Programs are tested before going into production, and change management procedures are in place. GLBA's Information Technology Policies and Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard	L/L	Low	Yes
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons		M/M	Medium	No
Integrity	Data could be entered incorrectly	Transaction journals are used. Contracts with third parties include language that addresses data integrity and service level agreements are designed to protect against this risk	M/L	Low	Yes
Integrity	Intentional incorrect data entry	Transaction logs are maintained and reviewed to detect incorrect data entry	L/M	Low	Yes
Confidentiality	Insecure e-mail could contain confidential information		L/H	Medium	No
Confidentiality	Internal theft of information	GLBA's Code of Conduct Policy	L/L	Low	Yes
Confidentiality	Employee is not able to verify the identity of a client, example: phone masquerading	Customer must provide the date of last deposit, or other confidential personal information within their file, and give to the employee before information is released	L/H	Medium	No
Confidentiality	Confidential information is left in plain view on a desk		M/M	Medium	No

Figure 4.25 FRAAP worksheet 4 acceptable risk level determined.

Confidentiality	Social discussions outside the office could result in disclosure of sensitive information	Code of Conduct/Conflict of Interest Policy. Annual Awareness item	M/M	Medium	No
Availability	Files stored in personal directories may not be available to other employees when needed	GLBA's management has established written policies and procedures to ensure information resources are available. See GLBA's Information Technology Policies and Procedures Manual No. 8-1 and Information Technology Policies and Procedures Manual No. 7-4	L/H	Medium	No
Availability	Hardware failures could affect the availability of company resources	GLBA's management has established written policies and procedures to ensure information resources are available. See GLBA's IT P&P No. 8-1 and IT P&P No. 7-4. Vendor maintenance agreements are established to support timely resolution of hardware failures. Files are imaged and stored to support recovery of information (Ghost files)	L/L	Low	Yes
Availability	A failure in the data circuit could prohibit system access	Vendor maintenance agreements are established to support timely resolution of hardware failures. See Information Technology Policies and Procedures Manual No. 2-2	L/L	Low	Yes
Availability	Act of God—tornado/hurricane		M/H	High	No
Availability	Upgrades in the software may prohibit access	GLBA's management has established written policies and procedures to ensure that software is tested before use in a production environment. See GLBA's Information Technology Policies and Procedures Manual 3-1 and IT P&P Manual 4-18	L/L	Low	Yes

Figure 4.25 (Continued) FRAAP worksheet 4 acceptable risk level determined.

- Gramm Leach Bliley Act (GLBA)
- Sarbanes Oxley Act (SOX)
- Information Security for Banking and Finance (ISO/TR 13569)
- FFEIC Examination Guidelines

For this example, we will be using a set of controls based on the IT organizations and groups that support the business processes. There are 34 controls that the team can select from. It is not necessary to try to select the one perfect control at this time. Remember, one of the goals of risk assessment is to record all of the alternatives that were considered (Figure 4.26).

The team will be selecting controls for only those threats that registered as high risks (those with "high" or "medium" levels). Those threats with a risk level of "low" will be monitored for change. All possible controls should be entered into the FRAAP worksheet (Figure 4.27).

Control No.	IT Group	Control Category	Definition
1	Operations controls	Backup	Backup requirements will be determined and communicated to Operations including a request that an electronic notification that backups were completed be sent to the application System Administrator. Operations will be requested to test the backup procedures
2	Operations controls	Recovery plan	Develop, document, and test recovery procedures designed to ensure that the application and information can be recovered, using the backups created, in the event of loss
3	Operations controls	Risk assessment	Conduct a risk assessment to determine the level of exposure to identified threats and identify possible safeguards or controls
4	Operations controls	Antivirus	(1) Ensure LAN Administrator installs the corporate standard antiviral software on all computers. (2) Training and awareness of virus prevention techniques will be incorporated in the organization IP program
5	Operations controls	Interface dependencies	Systems that feed information will be identified and communicated to Operations to stress the effect on the functionality if these feeder applications are unavailable
6	Operations controls	Maintenance	Time requirements for technical maintenance will be tracked and a request for adjustment will be communicated to management if experience warrants
7	Operations controls	Service level agreement	Acquire service level agreements to establish level of customer expectations and assurances from supporting operations
8	Operations controls	Maintenance	Acquire maintenance and/or supplier agreements to facilitate the continued operational status of the application

Figure 4.26 FRAAP controls list by IT organization.

9	Operations controls	Change management	Production migration controls such as search and remove processes to ensure data stores are clean
10	Operations controls	Business impact analysis	A formal business impact analysis will be conducted to determine the asset's relative criticality with other enterprise assets
11	Operations controls	Backup	Training for a backup to the System Administrator will be provided and duties rotated between them to ensure the adequacy of the training program
12	Operations controls	Backup	A formal employee security awareness program has been implemented and is updated and presented to the employees at least on an annual basis
13	Operations controls	Recovery plan	Access sourced: implement a mechanism to limit access to confidential information to specific network paths or physical locations
14	Operations controls	Risk assessment	Implement user authentication mechanisms (such as firewalls, dial-in controls, secure ID) to limit access to authorized personnel
15	Application controls	Application control	Design and implement application controls (data entry edit checking, fields requiring validation, alarm indicators, password expiration capabilities, check-sums) to ensure the integrity, confidentiality, and/or availability of application information
16	Application controls	Acceptance testing	Develop testing procedures to be followed during applications development and/or during modifications to the existing application that include user participation and acceptance
17	Application controls	Training	Implement user programs (user performance evaluations) designed to encourage compliance with policies and procedures in place to ensure the appropriate utilization of the application
18	Application controls	Training	Application developers will provide documentation, guidance, and support to the operations staff (Operations) in implementing mechanisms to ensure that the transfer of information between applications is secure
19	Application controls	Corrective strategies	The Development Team will develop corrective strategies such as reworked processes, revised application logic, etc.
20	Security controls	Policy	Develop policies and procedures to limit access and operating privileges to those with business need
21	Security controls	Training	User training will include instruction and documentation on the proper use of the application. The importance of maintaining the confidentiality of user accounts, passwords, and the confidential and competitive nature of information will be stressed

Figure 4.26 (Continued) FRAAP controls list by IT organization.

22	Security controls	Review	Implement mechanisms to monitor, report, and audit activities identified as requiring independent reviews, including periodic reviews of user IDs to ascertain and verify business need
23	Security controls	Asset classification	The asset under review will be classified using enterprise policies, standards, and procedures on asset classification
24	Security controls	Access control	Mechanisms to protect the database against unauthorized access, and modifications made from outside the application, will be determined and implemented
25	Security controls	Management support	Request management support to ensure the cooperation and coordination of various business units
26	Security controls	Proprietary	Processes are in place to ensure that company proprietary assets are protected and that the company is in compliance with all third-party license agreements
27	Security controls	Security awareness	Implement an access control mechanism to prevent unauthorized access to information. This mechanism will include the capability of detecting, logging, and reporting attempts to breach the security of this information
28	Security controls	Access control	Implement encryption mechanisms (data, end-to-end) to prevent unauthorized access to protect the integrity and confidentiality of information
29	Security controls	Access control	Adhere to a change management process designed to facilitate a structured approach to modifications of the application to ensure appropriate steps and precautions are followed. “Emergency” modifications should be included in this process
30	Security controls	Access control	Control procedures are in place to ensure that appropriate system logs are reviewed by independent third parties to review system update activities
31	Security controls	Access control	In consultation with Facilities Management, facilitate the implementation of physical security controls designed to protect the information, software, and hardware required of the system
32	Systems controls	Change management	Backup requirements will be determined and communicated to Operations including a request that an electronic notification that backups were completed be sent to the application System Administrator. Operations will be requested to test the backup procedures
33	Systems controls	Monitor system logs	Develop, document, and test recovery procedures designed to ensure that the application and information can be recovered, using the backups created, in the event of loss
34	Physical security	Physical security	Conduct a risk assessment to determine the level of exposure to identified threats and identify possible safeguards or controls

Figure 4.26 (Continued) FRAAP controls list by IT organization.

Threat	Existing Control	Select New or Enhanced Control(s)	New Probability/ Impact	New Risk Level	Acceptable Level (Yes/No)
Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons	Information classification policy in place. Information handling standards are being developed	Information classification policy in place. Information handling standards are being developed	L/M	Low	Yes
Insecure e-mail could contain confidential information	Information handling standards are being developed. Concern to be addressed in GLBA's employee awareness program and new employee orientation	Information handling standards are being developed. Concern to be addressed in GLBA's employee awareness program and new employee orientation.	L/M	Low	Yes
Employee is not able to verify the identity of a client, example: phone masquerading	In addition to existing controls. Concern to be addressed in GLBA's employee awareness program and new employee orientation. Continue to monitor	In addition to existing controls. Concern to be addressed in GLBA's employee awareness program and new employee orientation. Continue to monitor	L/M	Low	Yes
Confidential information is left in plain view on a desk	Information handling standards are being developed. Concern to be addressed in GLBA's employee awareness program and new employee orientation	Information handling standards are being developed. Concern to be addressed in GLBA's employee awareness program and new employee orientation	L/M	Low	Yes

Figure 4.27 FRAAP worksheet 5 showing additional controls and new risk levels.

Threat	Existing Control	Select New or Enhanced Control(s)	New Probability/ Impact	New Risk Level	Acceptable Level (Yes/No)
Social discussions outside the office could result in disclosure of sensitive information	Code of Conduct/Conflict of Interest Policy. Information handling standards are being developed. Concern to be addressed in GLBA's employee awareness program and new employee orientation	Code of Conduct/Conflict of Interest Policy. Information handling standards are being developed. Concern to be addressed in GLBA's employee awareness program and new employee orientation	L/M	Low	Yes
Files stored in personal directories may not be available to other employees when needed	GLBA's management has established written policies and procedures to ensure information resources are available. Employee awareness program will reinforce the requirements	GLBA's management has established written policies and procedures to ensure information resources are available. Employee awareness program will reinforce the requirements. Verify compliance	L/M	Low	Yes
Act of God—tornado/ hurricane	Senior management to champion Business Continuity Planning program. The BCP will also drive Emergency Response Procedures and an IT Disaster Recovery Plan	Senior management to champion Business Continuity Planning program. The BCP will also drive Emergency Response Procedures and an IT Disaster Recovery Plan	M/M	Med	Yes

FIgure 4.27 (Continued) FRAAP worksheet 5 showing additional controls and new risk levels.

The FRAAP team must understand that trade-offs must be made between business objectives and controls. Every control or safeguard will affect the business process in some manner as resources are expended to implement the control. Accidents, errors, and omissions generally account for more losses than deliberate acts. No control can or should be 100% effective. The ultimate goal is to achieve an acceptable level of security.

The FRAAP will not eliminate every threat. Management has the duty to determine which threats it will implement controls on and which ones to accept. The FRAAP team is to assist management in making that informed business decision.

Using a Threat Identification Checklist

As we briefly examined earlier in this chapter, it is possible to use a checklist to help the team through the threat identification process. Appendix A contains a sample threat checklist and a sample procedure on how to use a checklist approach to risk management.

FRAAP Session Summary

At this point, the FRAAP session is complete. The team was given an overview of the risk assessment process and what will be expected of them. The owner then discussed the scope of the risk assessment and a technical support person reviewed the information flow model. The facilitator then walked the team through the review business attributes (integrity, confidentiality, and availability). Once all threats were identified and recorded, the team took a few minutes to edit and consolidate the threats. Once the consolidation was complete, the team examined each threat and identified any existing controls or safeguards in place. When that process was completed, the team examined each threat for the probability of occurrence and then its effect on the business process. The team examined each threat using the existing controls as a guide. The result of this activity was to assign a relative risk level to each threat.

Once the risk levels were established, the team then used a list of possible controls and identified possible controls that could reduce the threat risk level to an acceptable range. The team then did a probability and impact review of those specific threats to see if the new or additional controls would be effective. For each new control, the team identified either a person or group that would be responsible for the implementation of the control.

When this process is complete, the FRAAP session is complete and the meeting is adjourned. A total of four deliverables come out of the FRAAP sessions:

- Threats were identified
- Risk level established

- Compensating controls selected
- Control “owner” identified

Post-FRAAP Process

The FRAAP session will typically take the entire 4 hours scheduled for it. I like to take a break for lunch and then begin the process of creating the reports that afternoon. One important element that needs to be stressed is the presence of the scribe. This person (oftentimes, it is me doing both roles) will record the activities on the FRAAP as the 4-hour session is unfolding. Nowadays, I typically use my computer and a projector to show the risk action plan on a screen or wall in the FRAAP workroom. Using this, all of the threats and following decisions are recorded in real time. This allows the facilitator and scribe to begin the process of preparing the final documents.

In the movie *The Big Chill*, Jeff Goldblum plays a writer for *People Magazine* named Michael Gold. When they asked him what he wrote, he told them that it didn’t matter what he wrote, he just had to make certain that the length of the article was about the same time the average person spends in the bathroom. Here is a hint about the length of your Management Summary Report, it should be no longer than the average time an executive would spend in the restroom. That is probably where it is going to be read, so you need to be prepared.

The following Management Summary Report is put together in a format that I use. The components of the report will be consistent for the most part, but the order of things may change based on the culture and standards of your organization. The format I use is as follows:

- Title Page
- Table of Contents
- Attendee List
- Scope Statement Summary
- Assessment Methodology Used
- Summary of Assessment Findings
- Where to Obtain Full Documentation
- Conclusions

After the standards Title Page and the Table of Contents, I like to establish right away *who* took part in the FRAAP. This is a result of my early training in the business world in which typically the first question from management was to tell them who had been part of this process. When you read NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, they recommend that the Attendee List be attached in an appendix to the report. Neither style is right nor wrong, they are both correct based on the specific culture of the organization. When you prepare your Management Summary Report, be certain to abide by the norms of your organization.

One more thing about the Attendee List makeup. I have no qualms about identifying those individuals that had been invited but did not attend. This again is a cultural morass that must be explored and researched before attempting to include in the report.

A summary of the Risk Assessment Scope Statement is discussed next. This should be two or three paragraphs at a maximum and contain a high-level overview of what the assessment was. Include when and where the risk assessment was conducted. If there was a compelling reason to conduct the assessment at this time, then that should be identified here. Be sure to include any assumptions and or constraints that you feel affected the process.

A brief description of the actual risk assessment methodology needs to be part of the documentation. Spend a few brief paragraphs creating the picture of how the team reached the conclusions that it did. The full details documentation will provide the intricate details; here, an overview will be sufficient.

In the Management Summary Report, I like to take the top high-level risks and present them to management in a brief description and a visual to reinforce the discussion. This discussion will give a brief synopsis of the key high-level risks and what actions are going to be taken to reduce the risks to acceptable levels (Figure 4.28).

Risk Level	No. of Similar Threats	Description of Threat Scenario
A	4	Physical intrusion
A	2	Power failure
B	10	Information handling and classification
B	4	Password weakness or sharing
B	4	People masquerading as customers
B	3	Firewall concerns
B	2	Computer viruses
B	2	Workstations left unattended
B	2	Employee training
B	27	Individual threats identified

Figure 4.28 FRAAP Management Summary Report visual.

Risk assessment identified five key areas of concern:

1. Restricted physical access areas should be considered throughout GLBA
   Action Plan: A physical security risk assessment will be conducted to determine if there is a need to create restricted access areas and/or increase physical access controls.
2. Power failure could cause corruption of information or prevent access to the system
   Action Plan: Network UPS may not be adequate for a power outage out of regular business hours. Install a backup domain controller at Ualena Street and connect it to the Ualena Street UPS.
3. Information classification scheme is incomplete
   Action Plan: GLBA has created a draft information classification policy that addresses five categories: public, internal use, restricted, confidential, and classified. The new policy requirements are to be disseminated to the GLBA staff and will become part of the new employee orientation and the annual employee awareness program.
4. Concern that the weakness of passwords for some information systems user accounts could allow compromise of the password and permit unauthorized access to GLBA systems and information
   Action Plan: The GLBA Passwords Policy is to be modified to require strong passwords. GLBA ISD will investigate software solutions to enforce a strong password requirement.
5. Someone could impersonate a customer to corrupt or access bank records or accounts
   Action Plan: Concern to be addressed in GLBA employee awareness program and new employee orientation.

Finally, there is the Conclusion section. Here, you can wrap up the overall process and tell management that the issues of risk are being addressed. Here too is the place where you can identify those risks that the owner decided to accept. This would also be the place where any constraints that affected the results of the risk assessment process should be identified.

During the risk assessment process, sometimes issues that are beyond the scope of the assessment under review rise to the surface. The Conclusion section offers a vehicle to identify and have these issues addressed.

As you complete the Management Summary Report, you will be faced with the question of whether or not the report needs to be published. This again is a cultural issue. Two corporations that I have worked for required only that the report be published.

The risk assessment report and documentation is a lot like an audit report. Typically, both sides work together to uncover deficiencies and then both work to establish a mutually acceptable solution. When putting together the report documentation, the facilitator works directly with the owner and project lead to determine the best course of action and the timeframe for compliance. In the cases in which both sides work together, the publication of the report may not require a signature. Check with your management to ensure that the proper protocol is followed.

Complete the Action Plan

When last we left the FRAAP action plan, the worksheet contained the information shown in Figures 4.29 and 4.30.

The final element that must be determined is who will be responsible for the implementation of the new or enhanced control and when the task will be completed. The establishment of the timeframe for implementation will take a bit of

Business Attribute	Threat	Existing Controls	Probability/ Impact	Risk Level	Acceptable Level (Yes/No)
Integrity	Data stream could be intercepted	Vacant ports are disconnected	L/M	Low	Yes
Integrity	Faulty programming could (inadvertently) modify data	Programs are tested before going into production, and change management procedures are in place. Fred's Information Technology Policies and Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard	L/L	Low	Yes
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons		M/M	Medium	No

Figure 4.29 Post-FRAAP worksheet section 1.

Business Attribute	Threat	Existing Controls	Risk Level	New or Enhanced Control	Probability/ Impact	Risk Level	Acceptable Level (Yes/No)
Integrity	Data stream could be intercepted	Vacant ports are disconnected	Low				
Integrity	Faulty programming could (inadvertently) modify data	Programs are tested before going into production, and change management procedures are in place. Fred's Information Technology Policies and Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard	Low				
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons		Med	Information classification policy in place. Information handling standards are being developed	L/M	Low	Yes

Figure 4.30 Post-FRAAP worksheet section 2.

Business Attribute	Threat	New or Enhanced Control	Probability/ Impact	Risk Level	Acceptable Level (Yes/No)	Responsible Entity	Compliance Date
Integrity	Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons	Information classification policy in place. Information handling standards are being developed	L/M	Low	Yes	Information Security Team	Third quarter this year

Figure 4.31 Post-FRAAP worksheet section 3.

work. This information needs to be entered into the worksheet. I typically use an Excel worksheet and it gives me the flexibility I need to enter all of the information into one document (Figure 4.31).

The risk assessment is not complete until the paperwork is done. The action plan must have the threats identified, the risk levels established, and the controls selected. Once the controls have seen selected, the action plan must identify who will implement the control and by what date. If the management owner decides to accept the risk, then this action must be identified in the action plan and in the Management Summary Report.

Like all important tasks, the proof in how well it went lies in the documentation that supports the process. Remember, the results of a risk assessment will be used twice, once when a decision must be made and then again when something goes wrong. By having complete documentation, management will be able to show when the decision was made, who was involved in the process, what was discussed and what alternatives were considered.

Conclusion

Capturing the threats and selecting controls is important, but the most important element in an effective risk assessment process is establishing the risk levels. Before any organization can decide what to do, it must have a clear picture of where the problems are. As you will see in the next chapter, there are any numbers of ways to modify the risk assessment process to meet the organization's needs. The process requires that the facilitator be flexible and work with the owner to establish needs before the risk assessment process begins.

Appendix A contains a procedure that discusses an updated version of the FRAAP. The appendix includes the procedure process and a sample threat checklist that is currently being used throughout the industry.

Chapter 5

Building and Maintaining an Effective Security Awareness Program

John G. O'Leary

Contents

Overview

Technology is a wonderful thing. Security technology keeps improving. It makes our jobs easier and strengthens the security of our computers and communication resources. And some of the newer and more advanced technologies require little or no human intervention. But the bad guys are improving, too; and so is their technology, and it's doubtful that we'll ever eliminate the actions or effects of carbon-based life forms (that's us) in information security.

We've all heard of "security awareness" and we've all got some picture or notion of what that phrase means. Those initial notions, however, tend to be incomplete. Security awareness includes multiple activities and different approaches aimed at various levels of our organizations and seeking large-scale or subtle behavioral changes in addition to just being aware of particular threats. We must educate managers, users, and IT personnel on the importance of protecting information resources. Top managers need to know in macro the bottom-line terms. IT security professionals need detailed technical training. Computer users, application developers, and technicians must be shown what they can do on a day-to-day operational basis. This chapter tries to deliver practical ideas and techniques on how to tailor a computer security training/orientation program to diverse groups. We will cover how to *plan* a program. We'll see who needs to be involved in initiating the program, how to define target audience segments, what possible topics to focus on, and which meeting and presentation techniques are most effective. We'll also give some tips and techniques for dealing with management, whose support is crucial to the success of the program.

Overall Objectives of This Chapter

At the end of this chapter, students should be better able to plan, develop, and implement an effective, realistic, focused, and efficient security awareness program.

Specific Objectives of This Chapter

At the end of this chapter, students should be more able to

- Evaluate existing security awareness measures for applicability and effectiveness in their environments
- Ascertain specific IT security needs for different job functions and environments in their organizations
- Locate areas that need improvement to attain required levels of security compliance
- Identify realistic training options differentiated by content, costs, availability, vendor, and scheduling that will bring weak areas into compliance and prevent solid areas from becoming deficient
- Set priorities and implement the training and awareness program
- Understand principles and techniques for motivating people to perform the security-related components of their jobs well
- Analyze training content and technique alternatives for different audiences
- Determine ways to plan and sell computer security awareness programs within their organizations
- Examine ways of evaluating the effectiveness of their programs
- Identify ways of gaining support and compliance from the user community

To-Do's for Readers

Think in terms of relevance to your environment, now and in the future.
Remember that "workable" is more important than "elegant."

Chapter Outline

Terminology
Rationale
Making Awareness Happen
Targeting the Program
Needed Skills

Desired Outcomes
Group Culture
Program Content
    Factors
    Items
    Degree of Detail
Locating Resources and Information
    Internal
    External
Pinpointing Areas of Deficiency
Delivery Methods and Techniques
Special Events
Selling the Program
Dealing with Management
Maintaining Compliance

Terminology

The following is a partial list of terms relevant to the topic and comments on how to think of them in an "awareness" mode:

Awareness—cognizance. The realization that, in this case, both threats and countermeasures exist and that our organization is not automatically immune or untargeted. This is the "what" and the "why" that drives our need for…

Training—delivering techniques and explaining policies, products, and procedures. This is the "how" that ensures people at all levels can understand and perform the actions and use the provided countermeasures.

Education—what we really want to do. Awareness without training gets them all nervous and doesn't give them answers. Training without awareness doesn't give them the motivation to learn and learn well. We want to put our security measures and activities in the proper organizational context. An educated workforce is an extremely strong defense mechanism.

Motivation—getting buy-in. Convincing the targets of our awareness program that the measures we propose will really help, and that they should, therefore, actually do what we suggest and bring about some…

Behavioral change—this is the real measure for any security awareness program. In an effective program, the mental gear shifting is followed by changes in the way things are done. There's a little bit of a subtle difference here because the behavior we want to emphasize might be what they're already doing. If so, stress the security and operational benefits of staying the course and keeping alert. Behavioral changes we want to effect must be clearly delineated and explained in the context of how the people affected by the changes do their jobs.

Outcomes—did the suggested (or demanded) changes actually take place? And did they improve the security of the enterprise? Are they changing passwords more frequently and not using their dog's names? Have they learned how to operate and do they actually use the self-encrypting hard drives? Are they losing fewer laptops or handheld devices? And so on.

Deliverables—management wants to see concrete results. What are they getting for the money and resources they allow us to spend on this exercise? Keeping our outcomes tied to behavioral changes usually makes it easier to demonstrate some quantitative results. Focus on deliverables also helps us avoid becoming enamored of a technique or product that sounds wonderful but doesn't really improve our security. If it doesn't produce the desired effect, then it doesn't matter what a good deal we got or how nice the sales guy is or how minimally disruptive the run-time characteristics of the product are. Out it goes.

Targeting—although some elements of a security awareness program may be suitable for all users, there will always be specific groups whose needs don't fit the generics. Identifying the target audience segments is a crucial part of starting a program, and modifying the target segments as business needs and security realities change is an equally important function in an ongoing program. The security message must also be crafted for the particular target segments. That might mean slight or major changes in examples, delivery style, or emphasis.

Audience segments—these may be differentiated by size, location, or availability, but there should be a specific set of awareness and training objectives for each target audience segment. For "mixed" segments (e.g., all employees at location A, even though their security responsibilities are different) the topics and delivery must address the security needs of each subgroup represented in the segment.

Delivery vehicle—the mechanism chosen to get the message across to the target audience. Among the most used are

- *Briefing*—please don't make it a 4-hour "brief"ing.
- *Formal presentation*—usually for upper management. Spelling and grammar are crushal…er, cruscial…er, crucial. Errors will be noticed much more than the content.
- *Lecture*—not used very much, but good for techies needing to know the specifics of new technologies or the detailed workings of complex threat and vulnerability scenarios. Digging deep is encouraged.
- *Workshop*—put them to work and they'll get more out of the class. But make sure that the workshop situations reflect real-world possibilities and constraints. Too much blue sky and the exercise loses effect.

- *Seminar*—more relaxed, less formal. The focus here is on the exchange of ideas and building on the ideas of each participant. Better suited for long-term security items than immediate, pressing issues.
- *Case study*—especially good if they're internal. Sanitize by using fictitious names because you don't want to embarrass anyone; just get the message across. Case studies of other companies or agencies must be clearly relevant to your shop.
- *Hands-on lab*—excellent for training on new security technologies, but the commitment in resources and people is very steep. There must be monitors in the room to make sure that no one falls behind the pace of the primary instructor and that everyone in the class understands not just what to do but why this step follows that one. Equipment used should mirror what people will use in a production environment and be kept up-to-date.
- *Theme*—a catchphrase or motto or some unifying element that lets people know that this message, video, trinket, or sound bite came from and is associated with information security. Fairly common ones include "You are the key" and "Security begins with you." You can certainly be more creative.
- *Logo*—may be a certain typeface, mascot, created cartoon character, or color combination for messages. Again, as in the theme, we want something that clearly identifies the communication as emanating from and being about information security.
- *Reinforcement*—exercises or examples to strengthen the original security message. Hitting your point from several angles and several ways makes it much more likely to be remembered.
- *Effectiveness measurements*—these must be related to the behavioral change objectives of the program. Management wants to know if they're getting bang for the buck. Is the awareness program making us more secure?
- *Organizational culture*—this is especially evident and influential in larger organizations, but it can also rear its head quickly in small- to medium-sized organizations. If awareness thrust or a security program seems well thought out, reasonable, and effectively managed yet still gets poor results, look for some aspect of the program to be violating organizational culture. The culture might not be explicitly stated or published, but it will permeate the entire enterprise.
- *Group norms*—they might be related to organizational culture or to the dominant profession in a department. They delineate acceptable behaviors and specify what one shouldn't do. All too often, our proposed security measures tread on some group norm and evoke surprisingly fierce resistance. We must learn the group norms before trying to change group behavior.

- *Dominant profession*—there are organizations dominated by engineers, others driven by marketing or sales; universities should have academics as a dominant profession. It's quite possible that different departments of an organization have their own dominant professions. Knowing what they are makes it much easier to tailor an awareness and training program.
- *Informal organization*—as opposed to the published organization chart, this refers to the people in departments who aren't listed as leaders, but whose example tends to be followed by other workers. An informal organization leader may be an executive assistant, an experienced line worker, even a part-timer. From an awareness perspective, identifying the informal organization and getting its leaders to buy into security plans can smooth the delivery and vastly increase the acceptance level of proposed changes.

Rationale

Why We Need Information Security

Organizations depend on networks and computers. Yours is no exception. Computers and multiple other devices of varying kinds store and process data and information, which *is* an asset and which *can be* critical or sensitive. Compromise or loss of information or inability to process it have associated costs.

- *Replacement*—costs associated with recovering or reproducing and restaging data and information so it is once again usable for business purposes. This is what usually gets listed as the cost of data loss, and it can be substantial, but it's not the full and final cost.
- *Availability*—because the data were unavailable at a certain time, we couldn't perform some actions that depended on it. Some of the actions may be contractually mandated or legally required and could lead to fines or lawsuits or other penalties. We may also miss chances for significant profit (see Opportunity).
- *Confidentiality*—are items that were supposed to be kept secret. If not, which ones got compromised and to what level? Who do we have to notify about confidentiality breaches? How do we tell them? What does it cost? What does it do to whatever trust relationship we have tried to build with that customer, supplier, or partner?
- *Integrity*—if someone unauthorized has been in a database, can we still trust the content? Integrity checks, run to make sure no unapproved or undocumented changes have been made, take time and resources.

- *Opportunity*—in addition to missing opportunities for profit, we'll usually assign our best people to investigate and clean up one of these incidents. That means that our stars are not working on future architectures or technologies or potential products, but digging around in the debris of an incident. We're not getting maximal use out of their talents.

  How much *information* gets lost in natural disasters?
  How much in terrorist attacks?
  How much credibility does an agency or company lose in a data breach?
  What do privacy breaches cost schools and private sector firms?

Good management (not just Sarbanes–Oxley or Basel III, or FFIEC, or SAS-70, or GLB, or ISO 27001, or ITIL or PCI DSS or whatever new regulations come along) demands *accountability* at several levels.

- *Customer*—should know what data they gave and when they were given. Should also have an idea of the value of individual pieces of data that can be aggregated into significant information.
- *Owner*—usually the creator of the data or the manager of the area where the data were created.
- *Trustee*—this is usually the IT group or the database group. They don't own the data, but they are entrusted with its care.
- *User*—the internal customer of IT who actually uses or manipulates (or both) the data for business purposes.
- *Guardian*—not just IT security. Whoever has access to the data has some responsibility for guarding it and keeping it from unauthorized disclosure.
- *Database Administrator (DBA)*—the responsibility here is not that of the owner, but to make sure that the data warehouse or database system maintains data integrity and that the data can be trusted.
- *Webmaster*—again, not usually the owner or creator of data, but responsible for seeing that web controls are adequate to protect what needs to be protected.
- *Administrator*—for accurate and timely implementation of access control to data as approved by the owner.

What Is "Awareness," Anyway?

It's what makes people feel, think, and do. The sensitization or feeling part is visceral, elemental, instinctual, and emotional. The education or thinking part is intellectual and mental. The training or doing aspect is physical and hands-on, related to employment. The bottom line in all of this is summed up in the following equation:

$$\text{Knowledge} + \text{motivation} = \text{behavior}$$

Why IT Security Awareness?

People are the biggest threat. We get crime by the discontented: errors by those who are careless, pressured, distracted, iPadding, iPodding, cell phoning, misconstruing, multitasking, desensitized, or socially engineered.

Computers, networks, and information are hard to control and manage. We have errors and crime occurring at the speed of light. We face complex and changing technology. The client/server revolution freed the users, but complicated the security professional's world by giving us not just distributed but also dispersed networks located in uncontrolled, user-managed areas and featuring minimal audit trails. In the second decade of the twenty-first century, we have wireless everything, ever-increasing connectivity, and devices that simultaneously get smaller and hold and do more.

Making Awareness Happen

Appoint an Awareness Team

We'll need a multidisciplinary team for several reasons. The problem is complex. Security is viewed as overhead, and rightly so. It also crosses lots of corporate turf. Even though there is inherent awareness of the need for and value of security, people in all departments have heavy workloads, and we need their support, expertise, and knowledge.

The makeup, level, and size of the security awareness team will also vary with different organizations. Among those to be considered for membership are

- Information Systems Security—obviously.
- Physical Security Manager—getting more important as sizes of devices decrease and capacity increases.
- Computer users—because we're going to ask them to change, they ought to be represented and have a voice in the changes.
- Recovery group representative—contingency planning and business continuity/resumption must be addressed.
- Training expert—for guidance on how to structure and deliver our messages.
- Specific area managers—for good examples and for those areas that really need substantial change.
- Legal—increasingly necessary in the age of compliance, but don't let them turn your team into a debating society. Might consider bringing legal in only when their advice and counsel is recognized to be needed by the rest of the team.
- E-commerce group representative—as more production applications become web-facing or web-based, their input and buy-in is critical.

- Web developer—it's a lot easier to build security into new web applications than to add it on when the app has gone into production.
- Human Resources—so that we assure adherence to policies and don't create ones that are unenforceable.
- Corporate Communications Group—these people know how to effectively get the message out to all corners of the organization in an effective and efficient way. Through in-house publications and communications directed at shareholders, customers, employees, etc., they can help us adroitly express our ideas.
- Other—depends on the organization.

Part of the reason to staff the team with people from various departments is to ensure that you tie plans to organizational goals. The objective is commitment plus some degree of standardization.

Translate Goals into Action Plans

Whether the awareness team is to be full-time or part-time, they need to translate goals into an action plan. To do so requires asking several questions:

- *Who needs security awareness training?* Managers, first-line supervisors, end-users, IT people, "all," contractors, part-timers, admin people, and so on.
- *How should they change?* Just what behavioral changes do we want to see in each target group?
- *What must be learned?* If they're going to change behavior, they probably need to learn a different way of doing something.
- *What techniques are best?* How do we get the new methods across effectively and efficiently?
- *How to sell and budget the program?* Obtaining and maintaining management buy-in and support are always challenges, and even if the initial support is strong, we can't assume continued funding.
- *When to implement?* Usually, the answer is "now," but sometimes it's wiser to wait until another large-scale project completes or reaches a definitive milestone. But we can't let the awareness efforts keep getting put on the back burner.
- *What to monitor and track?* It's easy to measure how many people attend the sessions or perform the computer-based training, but what we really want here is based on the behavioral objectives of the awareness program. Did we actually get the changes we were looking for?

Targeting the Program

A "generic" security awareness program sounds about as dull as it usually winds up being. To really reach a specific audience, to really get the behavioral changes needed to improve security in the organization, specific target audience segments must be identified, fine-tuned, and periodically adjusted as conditions and priorities change. Although there are no school solutions or etched-in-stone rules for determining who the target audiences are, here are some suggestions and guidelines.

Information Technology Providers—those who envision, develop, test, install, repair, patch, maintain, tweak, implement, remove, replace, explain, document, and answer questions and complaints regarding IT systems are definitely targets for the awareness program. And don't forget the people who audit and secure the systems. Different subsets of the IT provider universe will need different security elements emphasized, and the manner of delivery might be different. Techies usually need all the gory details, sometimes down to the code instruction level or how this query is parsed by this subset of that system. A quick overview won't do it for them. But if you start covering buffer overflow mechanisms and defenses with the IT help desk operators, you'll be able to watch a glaze form over their eyes, even if they're nodding their heads in seeming comprehension. These guys and gals want to know how to respond to user questions and what triggers indicate that the reported problem is, indeed, security related and should be referred to level 1, 2, or 3 in Department X or Y for resolution.

IT Customers/Users—this category includes almost everyone in the organization. These days, even the janitors are wired (more likely wirelessly connected) in. Anyone who interacts with information or information systems will need some grounding in appropriate information security concepts and procedures. If there's an "all" category, this is it. Here's where you might very well have security awareness and training elements that are applicable to everyone. Even so, the method of delivery might not be the same for "all."

Information/Data Owners—a crucial target audience; but sometimes it's hard to pin down who the "owner" of a specific piece of information is. This is especially complicated in the world of Storage Area Networks (SANs) and Network Attached Storages (NAS) and public or private or hybrid cloud structures, even though information ownership should have been clearly resolved before any migration to SAN or cloud or whatever. Once you do identify the owners, you must make them understand their significant security responsibilities. They generally decide who gets what kind of access to which sensitive information. To do this effectively, they need both a business and a security perspective. They'll probably be well-versed in the business vagaries, so we need to make sure we emphasize security and relate it to the business reality they already understand.

All Managers—the group of "all managers" will, no doubt, include some of the owners referenced above, but also those people up the chain who don't have a lot of contact with day-to-day operational information and procedures. However, the status of manager usually involves access to sensitive, sometimes highly sensitive material, and security mistakes by managers can be a lot more damaging than those by us working stiffs. Examples are all over the newspapers and nightly news. Managers also may get desensitized to the importance of specific information if they have it in front of them and talk with their peers about it for hours on end and for days, even months at a time. They'll normally recognize the need for reinforcement of "handling sensitive information" components of your awareness program, but the training must not be patronizing. These people didn't get where they are by being careless and unintelligent.

There are about as many ways to partition security awareness program audiences as there are organizations with a program, but here are a few more possibilities, outlined with possible subcategories into which you can assign specific people or groups

By computer knowledge
- Alpha-geek wizard—knows all, sees all
- Web-head, crypto-nerd, Mr. Forensics, etc.—deep knowledge in one or a few areas
- Competent technician
- Application guru—might not be a techie, but can make one application dance
- Fully functional user
- Infrequent user
- Neophyte
- "What's an applet?"
- Former technical manager—Caution! Can be very dangerous. Technical knowledge ages very quickly and not well. The tendency here is to overestimate technical prowess and demand higher access level than is needed for manager role.
- Multiple clouds implemented at home
- "Wireless device of the month" club
- Had RFID and GPS implanted in the dog… and on the kids

By organizational function
- Personnel administration
- Finance/accounting
- Production/manufacturing
- Marketing/sales
- Research/engineering
- Customer service
- Order fulfillment

Because this is a fairly common partitioning scheme, here's an example of how one organization—a bank—divided its awareness audience by organizational function:

- Demand deposits
- Commercial loans
- Trust

- Mortgage loans
- Investment banking
- Investor relations
- Tellers
- Audit

When partitioning by organizational function, some degree of additional slicing will almost always be required. Here, for example, is how one company breaks out their information technology function:

- Programmer
- Analyst
- Telecomm specialist
- Network technician
- LAN administrator
- IT security officer
- Manager
- Webmaster/web content developer
- Cloud implementer

In conjunction with or instead of organizational function, you can partition by organizational level, such as

- Senior executive
- Middle manager
- First-line supervisor
- Technician
- Business specialist
- Administrative assistant
- Clerical employee
- "The Masses"

The type/model of computer used can also be useful, but that changes so frequently that any example would be out of date before publication.

Employment status can be an effective delimiter, especially in an environment bound by multiple contractual and legal obligations regarding full-timers versus part-timers versus contractors, etc. Here's how one organization does that partitioning:

- Employee
- Contractor
- Temp

- Co-op student
- Consultant
- Outsourcing firm employee
- Competitor employee on joint project
- Service/product provider
- Customer

Once the partitions are delineated, the next step is to determine approximately how many people are in each category. There might be 12 or 14 senior managers and hundreds, even thousands, in the general user category. To tailor the message and delivery style for optimal effectiveness, the size of audience "chunks" has to be factored in. Audience availability and scheduling, especially for the higher-ups, can be closely related to the size of an awareness audience partition.

Needed Skills

The set of required information security skills for a particular awareness program target audience segment depends on several factors:

The job—how much and what type of information do they interact with and handle every day? How sensitive is the information they see and modify? What are the business consequences of an error or deliberate malicious act?

The environment—here, we're talking about the business environment and the technical environment. What programs are running on what types of machines? Where are the crucial data physically located? What are the generally accepted procedures for handling sensitive information in this industry?

Group culture—what drives this organization, and what sort of people work here? Is it an engineering-oriented firm, a service-based agency, a commodity manufacturer? Is there a primary group culture—engineering, customer service, marketing, financial services? Knowing the group culture will provide a significant advantage when deciding what techniques to use in the awareness program.

Management—have they truly bought into the need for security and an awareness program? Do they follow the rules they approve for others? Do they understand the risks?

We often tend to classify our users as "generic," but those generic "users" perform very specific business tasks using computers: things like accounting, order entry, production scheduling, long-term planning, product design, customer service, market analysis, and a host of other necessary business activities.

Many use the computers and networks to perform several, usually interrelated, business tasks:

- Payables and general ledger
- Receivables and general ledger
- Order entry, parts inventory, JIT scheduling
- Sales results and marketing plans
- R&D testing and new product plans

Even though people are using the same basic application types, including spreadsheets, Word processors, project planners, database engines, messaging networks, etc., the *security ramifications* of what they do with these tools and specifically developed products and processes vary widely. That is what we must focus on when constructing a security awareness and training plan for our organizations.

Generally speaking, the more sensitive and valuable the data that people in a specific job work with, the higher the degree of security required. Security skills in a visible, critical position must go far beyond the awareness level.

Here's a partial list of security skills that may be required for people working in your organization. Add or subtract from the list as you see fit:

- For actual or potential incidents
  - Prevention
  - Recognition
  - Response
  - Containment
  - Event correlation
  - Collection of relevant data
  - Reporting
  - Remediation
  - Cleanup(?)
  - Retraining
- Social engineering analysis and defense
- Desktop security
- Password discipline
- Physical security
- Privacy protection
- Wireless connection discipline
- Classified item markings and handling
- Compliance analysis
- Internet taboos
- Criticality recognition
- Recovery procedures
- Evidence collection and handling
- Threat identification
- Off-site security procedures

Desired Outcomes

Security awareness programs are aimed at producing behavioral change or reinforcement. To measure the program's effectiveness, we need to know what the desired change was and to what extent it was completed and internalized. Therefore, among the first questions to be addressed when implementing a program are "What specific behavioral changes are objectives of the security awareness program at this organization? How do we want people to change? How do we know that they've changed?" These are not always easy to answer, but there are some change category indicators that can help tell us if the program's desired effects are taking place.

- Change category indicators for *training*
  - More frequent password changes
  - More designed-in security features
  - Fewer errors
  - *Use* of provided features
- Change category indicators for *education*
  - Better password control
  - Understanding of data value and sensitivity
  - Security budget increases
  - More security problems reported
  - "Better" audits
- Change category indicators for *sensitivity*
  - Less fear of new devices
  - Better attitudes toward security
  - Better feel for the risks
  - Acceptance of security measures
  - Suggestions for improvements in security
  - More questions asked
  - Others(?)

Group Culture

Group culture determines "allowable" behavior for members. It rewards conformity with group norms, whether or not they match organizational policy or sound security principles. Attempts to change the group culture invariably meet resistance. Challenges to group cultural norms tend to bring some form of punishment. Resistance to change can be minimized if the change accentuates a firmly held group value. The informal organization is often more important to address than the formal organization as it appears on a chart. Effective training must comprehend the differing group cultures within an organization to strike responsive chords. Change threatens informal power structures. Co-opt the informal organization leaders. If they buy in, others will follow. Profession culture is sometimes part of a group culture, sometimes a separate variable. Profession culture can be a major component of the overall corporate culture. Several group or profession culture conflicts tend to arise in organizations:

- Engineers versus marketers
- Everyone versus bean counters
- Private sector versus public sector
- Techies versus users
- Security versus technicians(?)

Some professions have been notoriously difficult for security practitioners to work with:

- Physicians
- Research scientists
- Engineers
- Customer service reps
- Computer/network wizards
- University professors

This can be an issue wherever there is some preponderance of specialists. Security training must be cognizant of the profession's norms, ethics, and ways of doing things

Network designers want technical details
  - How a security mechanism works
  - Resource requirements
  - Interfaces
  - Run-time characteristics
  - Reality, not speculation
  - Imprecise information will destroy your credibility

Sales reps want deal-closing leverage points
  - How will this affect the customer?
  - How can I sell it as a benefit?
  - How does it differentiate us from competitors?
  - No gory technical details
  - Simple explanations
  - Pictures

Program Content Factors

We're making progress. We've chartered our organizational awareness team, identified our audience segments and put some preliminary numbers of people in each segment. We've decided how we want their behavior to change and have at least some clues as to how we'll detect that change. Now, we must flesh out the program with appropriate content. The content for an information security awareness program varies widely and several factors affect this variation:

- *Organizational needs*—this should be the prime determinant for the content of the program. The difficulty is in pinpointing which organizational needs are most pressing, and the answer, all too often, is determined by internal politics rather than rational analysis. Nevertheless, someone in the higher echelons of management will usually give information security some guidance regarding what areas to address (data loss prevention, access control, incident response, social engineering defense, smart phone security, etc.) and this will point to definitive content.
- *Audience segment*—how big is the segment (dozens or thousands), how geographically dispersed are they? Can we effectively get the message to them without dispersing security people to the winds? How available are they to participate in the training? How big a time chunk do we get with them? Are they techies, business types, managers, IT people? Does the organization's assessment of the segment's security needs match the perception of those in the segment? If they don't think they need the training, its chance of success plummets.
- *Time parameters*—when should the awareness training program start? Right now, next week, in 6 months, after the Oracle conversion? We know how important security is and how necessary this awareness program is, but can we stop in the middle of the CEO's pet project to march everyone on the project through our course? Maybe we can hit them with part of the full curriculum now and save the rest for after project completion. Maybe the CEO thinks like us and wants security baked into the project implementation.
- *"Hot buttons"*—this wasn't a major issue when we planned and started the awareness program, but news stories or television/Internet coverage on foreign government hackers or damaging data leaks or inadequate recovery procedures or Stuxnet-type malicious code attacks or whatever have gotten management heavily focused on one area that absolutely, positively must be addressed in our awareness program…right now. Please understand that this is not optional. When upper management experiences a hot-button item, we must react. And, yes, that means that something that we were going to do, something that was decreed an organizational need, will have to wait while we re-aim the awareness training to counter the hot-button issue.
- *Budget*—it's not unlimited. We're competing with other departments for scarce budgetary resources, so we've got to make the most out of what we get. Search internally for help with a topic before going outside to buy a product or for some consulting. But try not to skimp on something that really is an organizational need.

- *Availability of awareness resources (including personnel)*—some content lends itself to self-study and little interaction with information security personnel. Some audiences prefer to take the bull by the horns and not be guided by security people as they learn what to do and how and why. In such situations, we can make our content available internally and track usage without a whole lot of hand-holding, question answering, and site visits. However, some content requires and some audiences want to be shown via hands-on demonstrations exactly how the new security mechanisms work and what to do if they don't work and what needs to be entered if this error message appears, etc. One-on-one training can actually be efficient for managers, especially upper managers, but it won't work for an army of general users. Just as our budget is not unlimited, neither is our supply of people to deliver the awareness training.

Program content must be consistent with both organizational requirements and employee personal goals. To avoid justifiable grumbling and lingering resentment toward information security, we must make sure that we inform them before they are held accountable and explain why controls are needed and why particular ones were selected. We'll get more and better cooperation if we express ideas in terms meaningful to the particular audience. It also helps if we can show how the controls we're proposing can prevent problems that they have experienced. One more caution—don't ignore the effect on their productivity. We will slow them down. Security controls do add steps to their normal routines. Don't deny it or gloss over the operational effect. Instead, focus on the long-term, and how these security controls can prevent future problems or keep them contained and manageable.

Program Content Items

Policy—policies, procedures, standards, and guidelines are all valid topics, but don't bore them to tears. Don't forget to mention the teeth in policies—that violations may have severe consequences. In awareness contexts, we usually stress positives, but for policy violation consequences, we need to let employees know that the consequences are real and that they might be quite unpleasant. It might help to quote from the organization's policy manual that "…violators may be subject to disciplinary action up to and including termination. The company will also fully cooperate with law enforcement regarding possible prosecution." If there have been violations in the past, then a history of enforcement accentuates the seriousness of the issue.

Threats—the specifics change constantly, but focusing on the threats' effects on job functions will keep them interested. Technical people will want and need details of perimeter incursion methods, stealth techniques, and damaging payloads. If there are available countermeasures, describe them. Tell them how to use the controls provided, where to get help, how to recognize an incident, how to report an incident, how not to destroy evidence, or how to recover from a problem. If relevant to the audience segment, describe pass-through attacks and possible contingent liability.

Horror stories—they've been a staple of awareness programs for decades, but must be used with considerable caution. Horror stories are certainly easy to find. It often seems that every day we see reports of a new data breach, hacking exploit, or lost device chock-full of sensitive information. However, if a story about industrial espionage is not relevant to the environment and specific target audience of our program, it won't move the program along toward the behavioral goals we're looking to accomplish. If the description of a massive power outage following the Supervisory Control and Data Acquisition (SCADA) system attack doesn't seem plausible to our employees, it won't register with them. Acts of God—fires, floods, storms, lightning—tend to be credible, but we have to make a stronger case for horror stories revolving around privacy violations or unapplied patches. We can use internal incidents but, once again, caution is strongly advised. Be careful about airing dirty laundry or embarrassing someone who survived the debacle. For internal incidents, stress successful recovery and praise those who did things right. For any of horror story, lay out the plan for using it in the program. Decide which target group(s) could benefit, how to slant the story to be meaningful to them, how much time to spend on it, what format to use to deliver it, what the primary message is, and what we want them to do or stop doing or do differently.

Rewards—true or not, the perception of most employees is that we in security are always trying to find people doing things wrong so we can admonish them. Rewards for people caught doing the right thing can help change this image and let those receiving the awards know that their efforts are appreciated. Verbal rewards in a public setting, maybe with a plaque and citation to go into the employee's permanent record, build goodwill and show that security can say thanks and that employees can make a difference. Certificates, mugs, pens, t-shirts, and assorted goodies can also be used as rewards. If the budget permits, attendance at a class or conference makes a strong positive impression, and the word gets around the organization quickly that these security guys can hand out some valuable stuff if you support their efforts.

Penalties—the other side of the coin for awareness programs is to cover the things that might happen if one doesn't follow the prescribed procedures. The gamut of penalties might include verbal warning, written warning, loss of access, mandatory training, loss of pay, reassignment, demotion, termination, and prosecution. This isn't pleasant stuff, but it might be necessary to remind people in a particular target segment that their actions may have significant consequences. Try not to be too preachy when covering these penalties. The danger is that we'll sound too much like their old stereotype of security and reinforce negative images.

Legal ramifications—here, we're not talking about personal penalties, but the effects on our business of the laws in places where we actually do or are looking to do business. We most certainly want to get the legal department to help with this, although it has happened that legal's first indication that there might be issues came in an awareness briefing delivered by a security person. Federal, State, Provincial, County, and Municipal laws may all come into play. Criminal laws are slowly trying to catch up with technology, so our people need to know about developments in that sphere, too. If applicable to our firm, economic espionage laws are valid awareness program content. Cover the purpose, the requirements for relief and for protection of proprietary data, and the mandates that must be followed. Privacy laws vary widely by location, but their importance gets magnified every day. If there is a Chief Privacy Officer at our shop, enlist him or her to give input on this topic.

Current guidance and policy—duties and responsibilities regarding several security areas can be selected for delivery to particular target audience segments. Whether it be computer, network, workstation, Internet, web, communication, smart phone, wireless, physical, or laptop security, some group will need guidance in their duties and responsibilities.

Security procedures—people get so busy doing their primary jobs that they often forget or ignore or bypass the security procedures we know are necessary. Content of an awareness program can almost always include some coverage of security procedures such as

- Password handling
- Security labeling
- Logging procedures
- Handling sensitive items
- Using security features
- PC practices
- LAN protection
- Network access and control
- PKI

Other potential topics

- Data integrity
- Information criticality and sensitivity
- Information accountability and ownership
- Quality control
- Risk management
- Contingency planning
- Physical security
- Personnel security
- Auditing
- Documentation

- Local union rules
- Merger partner security status and philosophy
- Outsourcing and security
- Telecomm and networks
- Security troubleshooting
- Where security resides
- Encryption
- Identity validation

The following is an awareness program topic list used by an actual agency. Based on their needs, budget, scheduling availability, and several other items we discussed earlier in this chapter, the agency decided to focus on their "Top 14 areas":

- Know your ISO
- Passwords
- Confidentiality
- Privacy
- Backup
- E-mail
- Viruses
- Incidents
- Cyber-security in infrastructure protection
- Social engineering
- Authorized use
- Privacy, security, and mission
- Computer disposal and confidentiality
- "Reply to all" on e-mail

Granted, there are a lot of topics listed, but not everyone got every topic. The "reply to all" on e-mails was actually aimed at two groups, which both seemed to think that this was standard procedure. In awareness presentations to other staff, the topic was barely mentioned, and produced some knowing smiles and head nods. The social engineering defense section was short for some of the audience segments but very detailed and example-filled for the help desk and for those who regularly interacted with the public. Everyone got schooled on how privacy and security fit into the mission of the agency, and everyone got some degree of coverage on passwords, incidents, and e-mails.

Degree of Detail

The preponderance of topics leads us to the next step in architecting an effective awareness and training program. For a specific topic and for a specific target audience segment, what degree of detail do we need to deliver? Several factors point to an answer for this.

Depth of coverage—how deep do we need to go on this topic for this audience? If they really don't need it at all, then *none* is the answer. If it's of interest to them, but not crucial, we can probably get by with *general* coverage, but still be ready to answer questions that may arise. If this is an area of significant concern to this audience, or if it should be, despite what they think, then we must dig deep and provide *detailed* coverage, replete with examples and explanations and whatever else it takes to make the security point, get them thinking seriously about the topic and effect the behavior changes we seek.

Duration of coverage—this will be based on the depth needed, as described above. But there are some other variables that affect duration. The complexity of the topic may preclude a 30,000-ft. view or mandate one. If the audience segment needs in-depth understanding, we must take the time to cover all the bases. Management doesn't want to read the code, and their eyes will glaze over if we start comparing encryption algorithm strength and methodologies. Audience availability is an important determinant of coverage duration. Shift workers and management are the most difficult to pin down for face-to-face training, and the time we get with them is always limited. Economics enters the picture when we're trying to get senior managers to allocate time for training on laptop security or use of encryption or some other procedural security item. Financial managers also view awareness training from a somewhat different perspective. To them, a one-hour awareness session with 40 people in a room is a person-week of productivity. Our training had better be to the point and worth the effort.

Locating Resources and Information

If the target audience universe is small, if we've got access to effective technology, if our staff in security is adequate in number and training competence, if we can handle describing technical threats and countermeasures as well as business and legal issues, and if we're not overburdened with other security tasks, then don't worry, be happy. We don't need help. So much for fantasy. We will need help; fortunately, there are many places where we can turn.

Internal Sources

Before we go outside to hire consultants or buy products or services, see who's knowledgeable and willing to cooperate internally. Sources for in-house expertise include

- Network designers
- Cloud implementation group
- System wizards
- Application gurus
- Virus response team

- Webmaster
- Users who have been hit
- Legal
- Training experts
- Audiovisual/communications group

Of course, this is only a partial list, but here is where being nice to one or more of the über-geeks can really pay dividends. Most internal people willingly participate with help and advice. Some will volunteer to give presentations or write scripts for others to present or white papers on favorite topics. Use them.

External Providers

We're probably not going to be able to get all the help we need internally. Reluctance, obstinacy, and competing commitments will see to that. So we then turn outward seeking enlightenment, guidance and help.

Local special interest groups—regional The International Information Systems Security Certification Consortium (ISC2), The Information Systems Security Association (ISSA) or The Information Systems Security and Control Association (ISACA) chapters, SANS mentor groups, etc.—generally are populated with professionals who are willing to both give and receive help. Joining one of these is an excellent move, not just for awareness reasons.

Security product vendors—yes, we know, they're going to try to sell us something or up-sell us on what we already have, but for once, we want to know what techniques they use to sell the product. After all, we're trying to sell the use of it internally.

Other users of the product—how did company A implement this, mesh it seamlessly with their other systems, and get it to run smoothly? Vendors will readily give us contact information for those who have successfully implemented whatever they're selling.

Web pages—if we dig, we can find a lot more than marketing material on some vendor web sites. Details, technical analyses, etc., are findable. On the other hand, for awareness purposes, maybe we want the marketing material.

Publications—security-oriented magazines, books, white papers, etc. Check Amazon, Barnes & Noble, etc.

Consultants—for specialized knowledge and for credibility with management.

Training firms—check their catalogs. Sometimes, the outlines for their classes can help you produce at least a partial training curriculum for a target audience segment on a topic of interest.

Membership organizations—American Society for Industrial Security (ASIS), ISC2, ISSA, ISACA, etc.

Universities—Norwich and others have specialties in information security at both graduate and undergraduate levels.

Pinpointing Areas of Deficiency

These are areas where inadequate security measures or lack of adherence to security procedures have caused or can cause significant negative business effects. Locating these areas provides not only justification for the awareness program but also indicates who needs what kind of training. Past experiences drive this process, as do both internal and external audit reports. Regulatory feedback, even anticipation of regulatory feedback, can move items up on the priority list, as can penetration testing results. Consultant security reviews and security assessment product results should also point to deficient areas, but sometimes internal politics will trump any reviews or assessments. We may not agree with a politically motivated list of deficiencies and associated awareness priorities, but we must remember that management foots the bill for the program and can reorder priorities as they see fit.

Standardized measurements based on

- ITIL
- NIST Publications
- SAS-70 (Now SASE-16)
- ISO standards
- COBIT
- COSO
- FIEC
- Basel
- PCI DSS

These can help us prioritize our program. The trick here is finding consistent standards. It's not that easy. With or without standards or assessment results, opinions play a major role in pinpointing areas of concern. Upper management has the final say, but we also may seek the opinions of area management, area workers, technical people, legal, the Chief Privacy Officer, the Compliance Group, or other security people. And don't forget that we're paid for our judgment. Our view might not be finally accepted as gospel, but our opinions on which areas need security shoring up is valuable.

Delivery Methods and Techniques

No matter how well we know our audience, how specific we can be regarding what they need to learn and what behavioral changes they need to make, how much great information we've collected to convince them to change their behavior (or keep doing what they're doing right)—unless we present it effectively—the desired outcomes won't be reached. As technology continues to increase its rate of change, and as people become more accustomed to newer and newer forms of technology, we are challenged not only to concoct strategies to secure the new stuff but also to use it for our awareness efforts, thus demonstrating secure use. Even so, some of the relatively ancient delivery technologies still work, and can work well if used properly and for the right topics with the right audiences.

We certainly can't cover all possible delivery mechanisms and techniques, but here is a sampling of ones that have been successful.

Presentations

PC projector—whether connected to a laptop or an iPhone or some yet-to-be-invented device, this has been the standard for quite a while. And it works, as long as it quickly and effectively hits the salient points and doesn't drag on (death by PowerPoint). And PC projectors keep getting smaller, cheaper, and more powerful, which means we can keep the lights on in the room and see the faces of the audience. This helps us identify and interact with those who have questions but might be reluctant to ask them.

Flipchart—an ancient technology, but still a good one. Draw pictures, list concepts, offer the marker to an audience member so that they can clarify their question or situation. Used well, it's an involving technology that gets people participating in the session.

Whiteboard—like a flipchart with automated storage and recall capability. Caution—don't use permanent markers.

Webinars—can reach a large and geographically dispersed audience. They can also be archived for later reference or for those who were busy during the live webinar.

Intranet Web site—if we can get a specialized security web site on the Intranet, so much the better. Presentations from multiple internal and external sources can reside here.

No A/V aids—lawyers can do very well speaking to a group with no audiovisual aids. Very few others can. And the longer the presentation, the more the attendees want something to look at or listen to in addition to the speaker.

New-hire orientations—this can be a great way to present a positive impression of security from an employee's first day. Keep it short, relatively light (don't stress episodes of people who've been terminated for security violations), and give them contact information for security. Emphasize how security can help them get rolling with their new ID and access permissions. Smile.

Department meeting presentations—everyone wins. They get to fill the agenda for a weekly, monthly, or quarterly meeting; we get the attention of a specific department so we can tailor our security message to fit their precise situation.

Board of Directors' presentations—board members might try to act casual, but for us as invited presenters, this is a very formal occasion. Make sure there are no spelling or grammar errors in the presentation. Make sure it's not too long or too geeky, but be ready to answer their "technical" questions.

Formal Security Courses

It might be a stand-alone course or a section of an existing class. If it's stand-alone, we might want different people from security or technical areas or user areas to cover different sections of the course. It could be focused on one product or one class of threats, or one critical issue. It might hit high points of weaknesses found in the latest security assessment and how to correct them.

If we can add a security component to an existing course, we might describe security add-ons that we've implemented for our use of the product. We can also cover how to use embedded or augmented security features. Use existing examples that are already in the course and tailor our security training to these examples. This minimizes the chance that we'll alter the flow of the class or contradict other class material.

Demos

Demos are great. Demos are dangerous. We can demonstrate threats, intrusion scenarios, mistakes, and accidents. We can show how easy it is to make a false assumption and proceed to open the door to our network. We can demonstrate countermeasures and show how they actually find and stop the probe or the attack. We can demonstrate to groups large or small, even one-on-one for senior managers. But to be effective, the demo has to work as advertised. We're not perceived as the brilliant, dedicated, courageous, dashing security gods we recognize in the mirror when we're fumbling around and rebooting and trying to get something to run and saying, "Gee, it never did that before." Therefore, here are four rules for demos:

1. Practice
2. Practice
3. Practice
4. Have a canned backup available to show what's really supposed to happen

Purchased Videos or DVDs

The purchased ones are usually divisible into segments, each emphasizing one primary security element. Total time for the purchased videos runs close to 20 minutes. This is not an accident. Security videos are not often Academy Award caliber. Our employees can handle maybe 20 minutes and still maintain some interest in the content, but beyond that, their minds wander. One way to avoid the 20-minute limit problem is to host "Brown bag theatre" sessions at lunchtime in a section of the cafeteria and show one or two segments of a video per session. It's important to also have a security person on hand to answer (or ask) questions. And get some discussion rolling.

Internal videos and films—this is a major effort. It needs pizzazz to maintain interest, but can't be too slapstick or too grim and somber. Scenarios must be believable. We've got to decide whether we're going to use employees or actors in the roles. Someone has to write a script, and the 20-minute rule applies here, maybe more than for purchased videos. Too many home-grown videos try to cover too many topics. We need to keep it focused. And we need to be ever-aware of costs. Really bad ones will find their way to YouTube and be there forever.

Routings of relevant articles—the keys here are threefold: not too many, not too often, and relevance must be direct and obvious. If the security message is appropriate, they can be articles about our organization, competitors, even companies in different industries if the parallels are real and visible. We can use horror stories or recovery sagas. This author prefers tales of recovery because they show that it's not just possible to get into a bad situation, but also to survive it.

Trinkets—with a security message and an identity logo. The object should be at least plausibly usable. A partial listing of the trinkets seen (and collected) by your humble correspondent follows:

ceramic mug	mouse pad	stickers	t-shirts
coaster	envelope opener	post-it notes	ball caps
squeeze balls	travel mug	memo pads	game tickets
wrist rest	candy jar	screwdrivers	carry-all bags
pen	paper clip holder	pencils	calendars
	yo-yo's	light balls	frisbees

White papers—these are detailed, security-related analyses of issues, threats, or future technologies that may be usable in your organization. Often, they are requested by management to address hot-button items. Sometimes, we'll generate them in anticipation of such a request. The main things about a white paper are that it is a detailed analysis, not an introduction, a glossing over, or a quick hit on a topic and it delves into the topic from the perspective and in the context of our organization. And whether its topic is cloud-related, mobile device, privacy, end point security, or anything else, start with a one-page summary for management, and then proceed with all the gory technical detail the subject merits. The one-page summary, though, must be clear and concise and not contradicted by the detailed analysis. If we get the help of respected techies on these, they can be surprisingly effective in convincing management that we do need some security-related piece of equipment or software or that we need to adopt some new policy or procedure.

Posters—make sure they are visually appealing and placed where clearly visible to the intended audience. Color helps, and regular rotation (at least monthly) prevents them from going stale. If we have a distinctive security logo, make sure it's prominent on the poster. Depending on the corporate culture, amusing posters can be good spurs to memory. However, please be careful using humor in posters because there are some people in high places who think that a light approach to security issues is highly inappropriate. A final caution—emphasize one message on the poster not a laundry list of security to-do's.

Guest speakers—expert speakers can bring interest to an otherwise dull discussion. Before going outside to hire a professional speaker on a security topic, check around inside the organization. We've probably got an expert somewhere in the technical group or legal or in one of the business groups who can not only cover the desired topic but also deliver the presentation from the perspective of our firm. Although sometimes, it does make sense to get an outsider to come in. The thinking is that the external expert has seen many more organizations and can bring a broader perspective to the topic. That expert should also be free from internal political influences, and therefore, should have no axe to grind. Security specialists can make very good guest speakers, as can motivators. Although with pure motivators, we must make sure that they know the security agenda we're trying to pursue.

Publications

Security awareness efforts are materially assisted by publications, whether they appear on paper or electronically readable form. Manuals for the security of existing applications can supplement inadequate vendor documentation. Guidelines can give examples specific not just to the organization but also to the awareness audience segment targeted. Reports let management and the rest of the firm know what happened during an incident or how we're doing in relation to goals and objectives. Pamphlets give quick coverage of an important issue. Bulletins and incident alerts provide an early warning system for serious threats.

Newsletters—there are some that we can buy from vendors, usually with some degree of customization allowed for our needs, but many awareness programs that feature newsletters build and publish them internally. There are two primary characteristics for security newsletters—short and regular. Don't try to produce a 16-page security newsletter monthly, or even quarterly. Two to four pages will suffice, and try to stress positive items rather than how someone in the organization really messed up. Mildly amusing incidents are okay, but don't embarrass any employees. The newsletter can also cover interpretations of laws, incidents, policies, etc. In lieu of writing a complete security newsletter, we can try to get a regular column in an existing "house organ" publication.

Intranet e sites—these have proven to be excellent resources for awareness and training programs. There are four primary objectives for a security intranet web site. And all of these objectives must be attained for the site to be successful:

- *Interesting*: if we put visitors to sleep, they won't come back
- *Relevant*: deal with our issues, not generic, blue sky, or some other firm's issues
- *Timely*: analysis of attacks from 2008 won't really help us. Keep information current
- *Protected*: if it gets breached, the embarrassment quotient is very high, and our credibility takes a major hit

There's no end to the things we can put on a security intranet web site. Among the more popular items commonly found are

- *Pointers and links to other items*: policies, articles, books, web sites, etc.
- Contests, quizzes, and prizes
- *FAQs*: this can save us a lot of time answering the same questions over and over
- Security survey forms
- Contact information for security personnel
  - Names
  - Phone numbers
  - Office location
  - Pictures
  - E-mail addresses
  - Areas of specialization
  - Backups: in case the primary person is unavailable

Policies
  Text
  Pointers
  Interpretation
  Examples
  Reasoning behind
  Draft new policies
  Solicitations for comments

Procedural guidelines—keyed to our specific work environments, with sequential steps and rationales, if possible

Security news—cull for things that are relevant to our organization

Incident bulletins/recaps/analysis

Security quarterly reports—with associated red, yellow, and green charts and dashboards

White papers—in all their glorious detail

Internal security job postings

Internal security newsletter

Details of horror and success stories—sanitize them to prevent embarrassing employees

Testimonials—from those who got hit by malware, made a mistake, or were socially engineered. If the person who experienced the problem is willing to describe it, this can be a very powerful training and attitude adjustment tool for others.

Reader comments (don't filter, except for language)

Incident reporting forms and instructions

Checklists (e.g., hacker incident response, possible virus, physical security incident, etc.)

Web-based presentations (e.g., "Getting Connected Securely," "Our Firewalls," "Using iPads Securely," "Smart Phones and Security at XYZ Corp.", etc.)

Recovery plan information—not heavy details here but an outline and where to go to find the details for different departments

Audit emphasis areas—if the areas know what audit will be looking at, and they shore up the security of those areas before the actual audit, it isn't cheating, it's improving the security of the organization

Even before we decide what will be included in our Intranet Information Security Web site, we should focus on the architectural elements, then the graphics. Please don't forget that users will not often visit someplace that features text, text, and more text. Think about what inducements we will offer to increase readership. Plan to prevent and recover from defacements. Decide whose help we'll need outside of the security department and how we'll get them interested in helping us.

Small Pamphlets and Booklets

These are almost always short and to the point. Successful ones have used card stock paper, colored stock, tri-fold sheets, and specially created odd-sized paper stock. They're dedicated to one topic, and give bite-sized nuggets of information to help users, managers, and technicians prevent and respond to problems. They also feature the security logo and motto (if there is one) and information on how to quickly contact IT Security. Among the topics that have been used for such publications are

- Local laws
- Securing sensitive information
- Things you should know and do when traveling with your laptop
- Systems security reference (what, where, and who to call…)
- Sarbanes–Oxley and you: a guide for managers
- Emergency procedures
- Desktop security handbook
- Administrator references

This is certainly not an exhaustive list. The possibilities are almost infinite here. Just remember to keep it short, interesting, colorful, and focused on specific dos and don'ts.

Formal Courses

If one or more formal classes on security topics are to be part of our awareness program, several items must go into the planning, implementation, and operational phases. Selecting topics and deciding on exact content comes first. Then, we must lay out a sequence and format for the course and decide whether we'll take material from existing courses or do unique development for this one. We've got to plan for resources, such as teachers, facilities, visual aids, handout materials, and possibly computers for each student. Depending on the duration of the course, we could need to schedule refreshment breaks or lunches (or both).

We've also got to determine

- *Timing*—what time of year or business cycle do we initiate and deliver the class?
- *Duration*—will it be 1 hour, a half-day, a full day, 3 days?
- *Frequency*—how often do we repeat it?
- *Scheduling*—who goes to which class when?

The topic, exact content, audience, and time available will help determine presentation style. We defined these back in the terminology section, so we'll just mention them here:

- Briefing
- Lecture
- Seminar
- Case study
- Workshop
- Hands-on lab

Sometimes, we'll decide to use a mixture of presentation styles, taking the best elements of several, perhaps adding some reinforcement exercises to augment learning.

There will be some additional resources we'll need for a formal course. Some easy to locate, others more complicated. Classrooms may be available at our site, but we may want to have the course off-site to minimize distractions and having students being called out of the class for trivial reasons. Scheduling classrooms becomes just as important as scheduling attendees.

Capacity—we'll need a room that comfortably holds the scheduled number of students, preferably with some extra size and chairs and tables for late sign-ups or people who missed the last iteration. For most classes, the configuration called "classroom," with a chair and table spot for each student and all facing the front of the room, will be just fine. But some seminars and classes featuring a great deal of interaction may be better served with the "U-shaped" configuration, teacher and projector in the opening of the U. On-site will no doubt be the least expensive location for the class, but scheduling gets complicated, and it has happened that a security class was told to vacate the room in the middle of the session because there was "an important meeting" that just got scheduled and needed a venue. If we go off-site, we need to budget for the room, A/V, refreshments, and possibly transportation of our people to and fro.

Hands-on labs can be very effective training solutions, but they're certainly not cheap. We'll need:

- Workstations
- Network connections
- Student IDs
- Scripted scenarios
- Extra instructors for monitor duty
- Specialized A/V

And for any formal class, if we're going to give the students a paper handout, we'll either have to develop it or contract out the development or buy a textbook that works for the class. If we want to reproduce some supplemental materials, we need to check copyright issues. If we want to add some relevant books (dead-tree or e-books) we'll need funds, lead time, and a logistics plan.

An *Intranet web course* or *quiz* can be an interesting awareness project. Some organizations that use them require passing the quiz to access the network. If so, make sure it's short and that security is available to help if someone thinks they should have passed and really needs to get to some data. A few considerations for an Intranet quiz:

- Who writes it?
- Who takes it?
- Needed score for passing?
- Grading? (Yes or No or P/F?)
- Maintenance—who keeps it up-to-date?

Special Events

Special events can energize a program. If done well, they show management's interest and raise the excitement level for everyone. An awareness event doesn't need to be elaborate, but it can allow the security team's creativity to manifest itself.

Campaign kick-off meeting—possibly off-site. One of the most effective ones this author has seen was held in a city museum that the company had rented for the day. Keep the pace up; make sure it doesn't drag. Be judicious in choosing speakers for the kick-off. We definitely want some C-level manager to start the festivities and show support. If budget allows, bring in an industry guru as a guest speaker. Focus on current, relevant issues and give a quick preview of planned awareness activities for the next year. Presentations may need to be repeated for shifts/office coverage.

Security awareness fair—these are more casual than the awareness campaign kick-off events, but they can feature more interaction for the target audiences. A security awareness fair might last 2 or 3 days and include displays (usually near cafeteria), security videos, vendor representatives, giveaways, contests with prizes, demos, and hands-on displays.

Security awareness day—same as the fair, but on a smaller scale. It's important that the event be informal and nonthreatening for the employees. Food helps (if you feed them, they will come), as do guest speakers from technical or business areas.

Road shows—logistically, these are more complicated, but they show the remote sites that they're not forgotten and that what they do really matters. Bringing the word to remote sites, even if it's the same general message demonstrates interest on the part of security. And if we use their people as guest speakers, we can tailor the message to the specific site, function, etc. It's also very important to encourage questions and answers.

Selling the Program

Unfortunately, information security doesn't sell itself. One of the first tasks for a security awareness program is convincing management and the organizational population that the effort is indeed necessary and fruitful. From the information security viewpoint, what we want is for information security to be a normal and accepted part of the organizational culture. There are some strategies we can use to achieve this.

Link to corporate goals—this is the absolute best way to ensure that there's a reasoned, adequate and coherent answer to the inevitable question "Why?" When we can tie an awareness event or thrust or subprogram (such as data loss prevention tools and techniques for those using web-facing apps) to a specific organizational goal (e.g., 30% of profit from web-based commerce by the third quarter next year), justification for the awareness effort becomes almost self-evident…almost. Linking to goals presupposes that we know what the goals are and when they get altered. It also means that we have to be ready to change our priorities when the goals are "readjusted."

Focus on the information asset—even though the threats might be to reputation or market position, our focus must be on the information asset and how compromises or damage to that asset can lead to negative consequences, or how effectively protecting and using information can help service levels or competitive advantage. Yes, we need to take the business perspective. But we must also explain to target audiences how the information we want them to protect affects the business. Focusing on the information asset also means emphasizing (and praising) what they're doing right so that they keep doing it.

Do at least a cursory risk analysis—it doesn't have to be formal, detailed, expensive, or time-consuming, but look around and analyze what's going on. Use your own experience as a baseline. Ask why things are done, and why this way, and what controls come into play, and who controls the controls, etc.

Check what others are doing—other departments or sites might be facing similar security challenges. Learn what to do or what not to do from them. Some unique characteristics in the target department or a compared one may make a control especially relevant or completely unusable. Competitors, even companies outside your industry, can also shine light on approaches to solving our problem.

Prepare for the future—last year's program might not be relevant this year and probably won't generate interest next year. Keep up-to-date with technology and business thrusts.

Understand their worldview—it's not limited to their department, but their main business focus is their department and how it fits into the organization's overall goals.

Speak their language—standard business English, not security geek talk.

Sell the benefits to them of the awareness program—of course, you must speak their language and understand their worldview to do this.

Dealing with Management

Without their support, there is no security awareness program. Managers have access to extremely sensitive material. It's possible for them to become desensitized to information's sensitivity. Managers also set the example, whether they want to or not. If they give only lip service to information security, it tells everyone else that the subject is not really important. This is one reason why management is such a crucial target audience segment for any awareness program. One-on-one training sessions might sound extremely profligate, but they could be a very effective mechanism for dealing with this target segment.

To get their support, use terminology familiar to them:

- Cost–benefit analysis
- Expenditures in terms of
  - Money
  - People

  - Resources
  - Payback and effect on mission
- Response to hot-button items (HIPAA, GLB, Sarbanes–Oxley, latest virus, terrorist defense, recovery, new laws, etc.)

“Required security skills” will depend on their judgment of how much security is necessary. You give input; they make the call. Handling sensitive information is usually an area where they’ll accept their need for training. However, their training can’t be long and drawn out. Avoid getting bogged down in technical details, but be prepared to answer their questions in terms of their reality. They don’t want themselves or the organization to be embarrassed.

Do not patronize them. This can be dangerous to both you and the awareness program. Managers didn’t get to where they are by being careless or stupid. They may not have information security expertise, but they know how the organization works and how to get things done. Management is generally receptive. They’re a good, responsive audience who will keep you on your toes. Be prepared to answer questions, and allow some sidetracking.

Politics will be unavoidable in any organization with more than two people. Even if some specific security skills are very obviously required, your saying so might be construed as stepping on toes or an attempt at empire building. You can make a career-endangering statement without even realizing it. Be aware of political realities where you work. Try to avoid being used as a tool. If possible, find an “angel”—someone in high places who shares your perceptions and opinions regarding information security and the firm. But even with an angel, there are sometimes unpleasant surprises. Don’t overreact when a political decision guts or hamstrings your carefully crafted, business-justified security awareness training plan.

Maintaining Compliance

To ensure continuing progress and avoid backsliding, we’ve got to put some steps in place to maintain compliance. Asking for suggestions can work remarkably well in resolving dilemmas and constructing compromises that provide adequate security and allow the work of the firm to continue with relative smoothness. Allying with audit helps them and us and makes the requests from both groups more consistent, giving less confusion to the general population. It also helps us follow-up for late-developing issues. Praise successes and those who help. We’ll get more cooperation down the road. Small security steps, rather than giant, traumatic leaps lessen the fear factor for those upon whom our controls get inflicted, and it’s easier to train people on small, gradual changes than massive upheavals.

Keep the program fresh by changing the style of delivery, the medium, or the particular message often. Consider the organizational culture; you’re not going to change it overnight.

Final words: communicate, communicate, communicate.

Bottom line—people will comply if they believe it's in their own best interest to do so.

Conclusion

Security awareness is a complex, multifaceted, ongoing, ever-changing, high-tech, and high-touch proposition. It is vital to our organizations… now and in the future. Real enthusiasm is the key.

Chapter 6

Physical Security

John A. Blackley

Contents

Data Center Requirements

The nature of physical security for a data center should be one of concentric rings of defense—with requirements for entry getting more difficult the closer we get to the center of the rings. Although company employees, authorized visitors, and vendors might be allowed inside the outermost ring, for example, only data center employees and accompanied vendors might be allowed within the innermost ring (see Figure 6.1 for illustration).

The reason for this is obvious—if we take a number of precautions to protect information accessed at devices throughout the organization, then we must at least make sure that no damage or tampering can happen to the hardware on which the information is stored and processed.

To take this idea of concentric rings of protection a little further, we should start by considering the data center itself. Is the building that houses the data center standing by itself or is the data center in a building that houses other functions? If the data center is in a dedicated building, what approaches are open to the building and how well-protected are staff as they enter and leave the building? We may want to start building a picture of the exterior of the building to show the "outer ring" of protection—including entrances and exits, car parking facilities, and lighting. This picture of the outer ring might look like the example in Figure 6.2.

Having said all that, the principle of consistency must still be applied. There is no point in building physical access controls at a cost of several million dollars if the potential damage that could be done to a data center is less than several tens of millions of dollars. Remember, the cost of controls must be consistent with the value of the asset being protected and the definition of "consistent" depends on what risks your organization's management decides to accept.

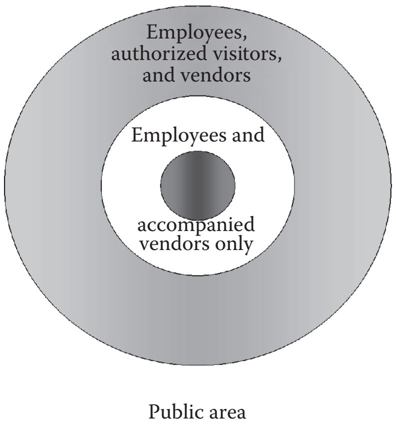


Figure 6.1 Concentric rings of protection.

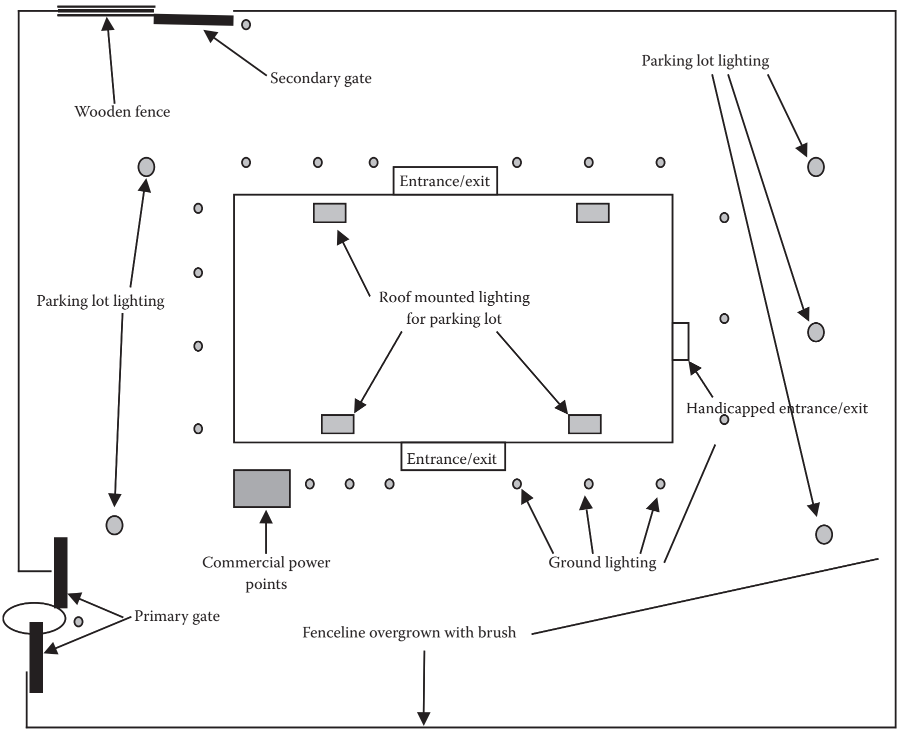


Figure 6.2 Outer ring of protection.

Physical Access Controls

When considering the physical access controls that are appropriate for (and consistent with) your organization, we must take into account a number of variables—including the assets to be protected, the potential threat to those assets, and your organization's attitude to risk.

Assets to Be Protected

Some organizations may decide to centralize operations and, in the course of doing so, build large, expensive "server farms" on their premises. On the other end of the scale, an organization might decide to take a decentralized approach and distribute their computers and computing equipment around the organization's many buildings.

The amount of effort put into protecting physical assets in both of the above scenarios might well come to the same total amount but would be spent on different forms of protection. For a large server farm, several concentric rings of technology-based protection and access control might be appropriate, whereas for the distributed version, simply keeping individual servers in locked rooms might be sufficient. This is one variation to be considered when choosing appropriate physical access controls.

Potential Threats

When assessing potential threats, a large dose of common sense is often our best tool. The threats that exist for high-profile commercial or politically sensitive operations differ very much from those faced by, say, a biscuit manufacturer. Likewise, an operations center located in the middle of a turbulent city will face a much greater threat than one sited in an industry park in a semirural setting.

We must also take into account the nature and recent history of the organization itself. For example, if the organization is a stable and long-established one with no history of employee strife, then the threat countermeasures (in the form of physical security measures) to be taken will be a lot fewer than if the organization does have a reputation for disgruntled employees and disruptive activity on the premises. This is a second variation to be considered when choosing physical access controls.

Attitude to Risk

Perhaps the most common complaint among information security professionals is that "they" don't understand the need for protective controls—"they" most often being management and senior management of the organization. Leaving aside the obvious rejoinder about it being the Information Security Professional's job to teach "them" about the need for protective controls, we must point out that it is the function of any organization's senior management to assess risk.

Daily business activities involve constant risk assessment. Every decision that is taken and that will influence how an organization does business involves a form of risk assessment in the act of making the decision.

It is no different with information security decisions. When facts and opinions have been made available to management and senior management, it is their function to decide on how risks will be managed. It is a fact of life that some organizations are very risk-averse and some are not. It is also a fact of life that individual managers have equally variable attitudes to risk. This is the third set of variation to consider when choosing physical access controls.

Sample Controls

Having looked at the complications involved in choosing appropriate physical access controls, it becomes clear that no "one-size-fits-all" solution exists. Each organization must examine its own particular assets, risks, and attitudes to risk before deciding on appropriate physical access controls. When that examination has been done, the organization will want to consider the following list of items when designing controls over physical access:

- Physical security protection for IT equipment and systems should be established—based on defined perimeters through strategically located barriers throughout the organization (already discussed at the start of this chapter).
- The security of the protection given must be consistent with the value of the assets or services being protected (already discussed at the start of this chapter).
- Support functions and equipment are sited to minimize the risks of unauthorized access to secure areas or compromise of sensitive information—for example, network engineers who will be called on often to enter the data center should not have their workplace located away from the data center.
- Physical barriers, where they are necessary, are extended from floor to ceiling to prevent unauthorized entry and environmental contamination. In other words, walls that are meant to prevent access, slow the spread of fire, or exclude dusty or polluted air must go all the way from the actual ceiling of the building to the solid floor of the building and not just from false ceiling to raised floor.
- Personnel other than those working in a secure area are not informed of the activities within the secure area. Although no one expects a cloak of secrecy to be hung over the existence of a data center or other sensitive operation, details of the business conducted inside a protected perimeter need not be known to anyone who does not have access inside the perimeter.
- Working alone and unsupervised in sensitive areas must be prohibited (both for safety and to prevent opportunities for malicious activities).
- Computer equipment managed by the organization is housed in dedicated areas separate from third party–managed computer equipment. Where a process or part of the organization's computing activity is carried out by a third party—that third party's equipment should be housed in an area that lets their engineers access the equipment without having access to the organization's computer equipment. This can usually be satisfied by keeping the two entities' equipment in separate cages in the same room.
- Secure areas, when vacated, must be physically locked and periodically checked.
- Personnel supplying or maintaining support services are granted access to secure areas only when required and authorized, their access restricted, and their activities monitored.
- Unauthorized photography, recording, or video equipment must be prohibited within the security perimeters.
- Entry controls over secure areas must be established to ensure only authorized personnel can gain access and a rigorous, auditable procedure for authorizing access must be put in place.

- Visitors to secure areas must be supervised and their date and time of entry and departure will be recorded.
- Visitors to secure areas are granted access only for specific, authorized purposes.
- All personnel must be required to wear visible identification within the secure area. The necessary addition to this is that we must foster a culture in which employees feel comfortable in challenging anyone who is in a secure area without visible identification.
- Access rights to secure areas are to be revoked immediately for staff members who leave employment.

Fire Prevention and Detection

Fire prevention and detection standards vary according to the premises—whether the premises also house materials or processes that increase the risk of fire and whether the premises themselves are located in an area where fire risk is higher or lower.

Generally, the local fire authority (Fire Marshall in the United States) can be consulted for advice on fire prevention and detection measures, and architects and vendors of data center equipment are also ready to give advice.

There are, however, some fire prevention and detection precautions that should be judged as standard and a minimum requirement for premises that house computers and critical information.

Fire Prevention

"No smoking" is the first rule. Although this is a common requirement throughout the United States at the time of writing, it is neither a Federal law nor a universally implemented State law. However, the use of smoking materials anywhere within a building that houses or processes critical information must be prohibited.

All flammable material—such as printer paper, plastic wrapping, and tapes—should be stored in an area separated from the main server or computer room by a fire-rated wall. Supplies for 1 day's processing can be kept in the server or computer room but larger supplies must be stored separately.

Flammable or highly combustible materials must also be kept out of such premises. Where an organization produces, uses, or transports hazardous materials, all such materials must be stored away from premises where critical information is stored or processed. Where janitorial staff use flammable or combustible cleaning solvents, they should also be stored off-site. If that is not possible, they should be stored in an area that is behind a fireproof door and that has its own smoke-detecting equipment.

Many organizations now find it prudent to limit the amount of electrical power used in each cabinet and cage in the data center. High use of electrical power creates a buildup of heat and creates the potential for the buildup of static electricity—both fire hazards. Ventilation and grounding are the keys, of course, to limiting the risk from these, but limiting the amount of electrical power used in any physical area also reduces the chance of a heat or static electricity buildup. Most designers of data centers recommend that the ambient temperature in data centers should not exceed 74°F (23°C) because that reduces the risk of such buildups and also eases the control of humidity within the room.

Of course, when controlling the temperature and humidity in an enclosed space, it is necessary to monitor them, and the system used to monitor temperature and humidity in a data center must have the following characteristics:

- The data gathered must be representative of the room being monitored. In other words, if only one sensor is used in the room, it is unlikely that a true picture of temperature and humidity will be available. Fluctuations from one part of the room to the next will not be detected and "hot spots"—unless they happen to occur under the sensor—will go unnoticed.
- The monitoring system must be capable of storing and presenting historical data. Seasonal and event-based fluctuations provide important indicators to how to manage temperature and humidity.
- The monitoring system must be able to provide alarms when temperature and humidity fall outside acceptable parameters. Fire, flood, or failure of the heating or cooling systems are all critical events and the monitoring system must be able to alert staff to their occurrence.

Fire Detection

The most common sources of fires in data centers are the electrical system or the hardware. Breakdowns in insulation and the resultant short-circuiting can lead to intense heat that can melt materials or cause a fire. Data center fires are often small or smoldering, with little effect on the temperatures in the room. Because the smoke itself can affect the computer hardware, it is necessary to employ a detection system that is sensitive to smoke and other products of combustion rather than temperature. The specific detection and extinguishing system is dependent on the specific design and exposures of the individual data center area. In the United States, National Fire Prevention Association (NFPA) 75 states that automatic detection equipment must be installed to provide early warning of fire. The equipment used has to be a listed smoke detection type and every installation of smoke detection equipment must be engineered for the specific area to be protected (giving due consideration to air currents and patterns within the space to be monitored).

Smoke and fire detectors should be wired to a central alarm panel that is continuously monitored and, ideally, is constructed so that any alarm given is repeated instantly at the nearest firehouse. Where permanent connection to the firehouse is not possible, an external alarm should be installed to allow people outside the building to be notified and to raise the alarm with the emergency services.

Firefighting

In data centers, as much damage can be done by the fire suppression equipment as by the fire itself. Nonetheless, effective fire suppression systems must be installed in data centers.

A passive system reacts to smoke and fire without manual intervention. The most common forms of passive suppression are sprinkler systems or chemical suppression systems. Sprinkler systems can be flooded (wet pipe) or pre-action (dry pipe). A flooded system means that the pipes are full at all times, which allows the system to discharge immediately upon detection. A pre-action system will fill the sprinkler pipes upon an initial detection, but will delay discharging until a second detection criterion has been met. Chemical total flooding systems work by suffocating the fire within the controlled zone. The suppression chemical most often found in data centers is halon 1301. Halon is being eliminated in favor of the more environmentally friendly FM200 or various forms of water suppression. Carbon dioxide suppression systems are also used, but can be a concern due to operator safety issues in the instance of a discharge. These can be used independently, or in combination depending on the exposures in the room, local ordinances, and insurance requirements.

The ideal system would incorporate both a gas system and a pre-action water sprinkler system. The gas suppression systems are friendlier to computing equipment. Water sprinklers often cause catastrophic and irreparable damage to the hardware, whereas the hardware in a room subjected to a gas discharge can often be brought back online soon after the room is purged.

Gas systems are, however, "one-shot" designs. If the fire is not put out in the initial discharge, there is no second chance. The gas system cannot be reused until it is recharged or connected to a back-up source. Water systems can continue to address the fire until it has been brought under control. Although this is more likely to damage the hardware, it is also a more secure means of protecting the building structure.

Water suppression systems are often preferred or mandated by building owners or insurance companies. Water systems are also highly recommended in areas containing a high level of combustible materials use or storage. The decision of what means of fire suppression to utilize must incorporate numerous factors, including the mission and criticality of the data center operations.

Verified Disposal of Documents

Although security precautions and fire prevention and suppression systems can ensure the safety of information within data centers, often little is done to protect information when it leaves the data center. Printed documents and documents on electronic media all leave the data center and, hopefully, fall under policies and standards for the protection of data throughout the workplace. But when documents are disposed of, all too often, the commonsense rules for protecting information are left behind.

We see documents clearly marked “Confidential” (or which, according to the content of the documents, should be clearly marked as such but aren’t) tossed into garbage cans and set out with the rest of the office rubbish. Where paper documents are collected, they are often left unattended—a convenient place for a wrongdoer to browse through a company’s paper output. In one facility I visited, the facility owners thoughtfully provided containers in which to dispose of confidential documents—large garbage cans clearly marked “Confidential Documents Only.” Once again, a convenient receptacle for wrongdoers to search.

It makes sense, does it not, that if we are to spend any money or effort to protect information, then the “circle of protection” ought to surround the information all the way to its destruction—and yet it so often does not.

Collection of Documents

The procedures for the collection of documents before their disposal should be documented and taught to all employees—and should avoid using large receptacles clearly marked “Confidential Documents Only.”

Every single department in the organization must have easy access to the containers used to dispose of documents. Where it involves more than a minute of time to properly dispose of a document, confidential documents will be put in garbage cans next to desks. Documents should be collected at fixed points in receptacles lined with opaque bags—so that, when the bags are taken away for disposal, the documents cannot be read through the bags themselves.

Where documents are collected in bins, we have to make a decision on whether or not to lock the bins. For locked bins, the advantages are that paper is secure (relatively) once deposited in the bin and we can demonstrate—to clients and auditors—that our information security circle of protection encompasses documents ready for disposal. Disadvantages include the procedures necessary to track keys, the extra expense, and the added attraction, for wrongdoers, of a locked (versus unlocked) document bin.

Clearly, every organization must make its own decisions on how to collect information destined for disposal and those decisions will be based on criteria already discussed in this book. One thing is certain, however, and that is this: If a secure document disposal process does not exist, then sooner or later, confidential documents will end up in the hands of someone who can use them to cause trouble for the company.

Document Destruction Options

There are three basic options for destruction of documents—recycling (commonly called pulping), shredding, and burning (although some organizations use a combination of one or more of these).

When considering recycling or pulping as an option, these factors must be taken into account:

- Recycling with a bonded service usually means contracting with a service to have the paper hauled to a bonded recycler or directly to a bonded paper mill. All of the paper sent to the recycler should be documented with shipping information and a Certificate of Destruction should be received to certify that the paper was sent directly to a specified locale on a specific date and was destroyed on a specific date.
- Where bonded recycling service is not available or is prohibitively expensive to use, we can perform an assessment of the recycler's procedures and facilities. If we find that recyclers handle and process paper in a manner that meets confidentiality standards for security, then we may use them instead of the more expensive, bonded alternative.

Shredding paper increases its volume and sometimes produces a false sense of security. Less-expensive shredders in fact only cut paper into ribbons that can be easily pieced together again and read. Even when we opt for a more expensive shredding option, we must consider these points:

- Although shredding can be an effective way of disposing of documents, it is also expensive and labor intensive, and if other options are available, it might not be necessary. Some organizations do their own shredding with small, departmental shredders whereas others choose to do it in a centralized fashion using a large, industrial centralized shredder.
- Some organizations also decide to minimize shredding on-site by working with a recycling hauler that provides secure services such as off-site shredding. These companies pick up the paper from a central point and either shred it on-site in mobile units or transport it to a bulk shredding facility. These firms come under the category of destruction firms, and they should always be able to provide a certificate of destruction.

Choosing Services

Document disposal and recycling functions are most often contracted services. However, the organization's responsibility for security of the documents does not end when they are removed from the facility. Making sure that the documents are subject to secure and reasonable processes until the information is destroyed is still the responsibility of the organization's facilities.

Agreements

Everyone outside the organization (which owns the documents) who is involved in the destruction of the documents (including waste haulers, recycling facilities, landfill, and incinerator owners) should sign an agreement that states that they know that they will be handling confidential information from the organization and they agree to maintain the confidentiality of the information. The agreement must limit the vendor to use and disclosure of documents and the information contained in the documents to those uses stated by a contract.

Contractual language protecting the confidentiality of the waste should be built into all contracts with solid waste and recycling haulers and include the following elements:

- Specify the method of destruction/disposal
- Specify the time that will elapse between acquisition and destruction/disposal of documents (or electronic media, if that is also to be disposed of)
- Establish safeguards against breaches in confidentiality
- Indemnify the organization from loss due to unauthorized disclosure
- Require that the vendor maintain liability insurance in specified amounts at all times the contract is in effect
- Provide proof of destruction/disposal

One final point to consider when deciding how to dispose of documents is their collection in a loading dock area. We must secure our solid waste compactors and containers by locking all accessible openings to the compactor. Metal doors can be welded on the compactors to allow for them to be easily locked. Ensure that the loading dock is secure at all times. The container for the documents and the loading dock itself must be designed to minimize or eliminate the risk of documents blowing around in the wind before or while they are being collected for disposal.

Duress Alarms

In many facilities, certain operations are carried out that place staff in positions of heightened vulnerability. For example, in a bank, tellers are at risk from criminals who rob the bank during business hours. In data centers, employees who handle negotiable instruments (checks, stock certificates, etc.) may also be at risk.

Where employees are performing jobs that increase the risk of their being vulnerable to coercion or attack, each employee's workspace must be provided with a duress alarm. The alarm activator (button or switch) should be placed so that it can be used without its use being noticed by others (a footswitch, for example, can be used without anyone watching being aware of its use).

The choice of whether the alarm should sound locally or not will be made on the assessment of the type of risk the alarm is meant to indicate. In other words, if sounding the alarm locally is likely to increase the risk to the employee setting off the alarm, then the alarm should not sound locally. By the same token, if a local alarm might bring help more quickly or alleviate the situation, then one should be installed.

Whether local or remote, all employees who might be called upon to respond to the alarm must be trained in response techniques and the response procedures must be kept up-to-date and stored at the place where responding employees normally work.

Intrusion Detection Systems

In the context of physical security, intrusion detection systems means tools used to detect activity on the boundaries of a protected facility. When we commit to physically protecting the premises on which our staff work and which house our information processing equipment, we should carry out an exhaustive risk analysis and, where the threat requires, consider installing a perimeter intrusion detection system.

The simplest intrusion detection system is a guard patrol. Guards who walk the corridors and perimeter of a facility are very effective at identifying attempts to break into the facility and either raising the alarm or ending the attempt by challenging the intruder. Of course, the most obvious shortcoming of a guard patrol is that the patrol cannot be at all points of the facility at the same time.

Which leads to the next-simplest intrusion detection system and that is video monitoring. We can place video cameras at locations in the facility in which all points in the perimeter can be monitored simultaneously and, when an intrusion attempt is detected, the person charged with monitoring the video surveillance can raise an alarm.

Purpose

Our first task in defining the requirements of an intrusion detection system is to define what is to be protected and what the level and the nature of the threat is. For general threats, we might ask: How does anything from the outside get to the inside? Are the parking lots secure? What is the mail delivery system? What is the environmental system exposure? What are the loading dock procedures? What building access controls exist?

Other questions to be asked in defining the purpose of the intrusion detection system relate to the history of the facility. For example, has there been a specific parking lot incident, grounds incident, or a property/facility trespassing incident? Are there general vulnerability concerns that may include trespass, assault, or intimidation? When was the last occurrence and what were the circumstances? Are the authorities aware and involved? Is there documentation available for review?

Answering these questions will help define what the purpose of our intrusion detection system is (and what it needs to achieve). The next task is planning the system itself.

Planning

Of course, both of the examples given above should have been chosen as the result of a need identified by a risk assessment plus careful planning. The planning should have been carried out with an objective to provide a solution that addresses

- Surveillance
- Control

- Maintenance
- Training

During planning, the nature of the facility and the contents of the facility themselves should be taken into account. For example, the intrusion detection systems' requirements for a dedicated data center campus, set in its own grounds and surrounded by a perimeter fence, differ greatly from those for a data center housed on the warehouse floor of a multistorey building in a city center.

Elements

The planning should produce a draft design that addresses the requirements of the premises. The elements of intrusion detection required will depend on the facilities—for example, the dedicated data center might require a perimeter fence, lighting on that fence and in the space between the fence and the walls of the facility, video cameras, and then the perimeter system for the building itself. On the other hand, a facility contained in a multiuse building will require intrusion detection systems on the doors, windows, floors, walls, and ceilings of only the part of the facility that contains the data center.

Elements to be considered when installing an intrusion detection system include

- Video surveillance
- Illumination
- Motion detection sensors
- Heat sensors
- Alarm systems for windows and doors
- "Break-glass" sensors (these are noise sensors that can detect the sound made by broken glass)
- Pressure sensors for floors and stairs

Procedures

Whatever tools or technologies are used in the intrusion detection system, the system will fail to provide security unless adequate procedures are put in place, and training on those procedures is given to staff expected to monitor and react to alarms created by the intrusion detection system.

Staff should be trained twice a year on what intrusion detection system alarms mean and how to respond to them. Those staff responsible for monitoring intrusion detection systems must be taught to recognize intrusion attempts and how to respond according to a response scale (i.e., when it is appropriate to respond in person, when to respond with assistance from facility personnel, and when law enforcement should be called for assistance).

Physical Security

Policy

It is the responsibility of the Company management to provide a safe and secure workplace for all employees.

Standards

- The Company offices will be protected from unauthorized access.
- Areas within buildings, which house sensitive information or high-risk equipment, will be protected against unauthorized access, fire, water, and other hazards.
- Devices, which are critical to the operation of company business processes, will be identified in the Company Business Impact Analysis (BIA) process and will be protected against power failure.

Responsibilities

- Senior management and the officers of the Company are required to maintain accurate records and to employ internal controls designed to safeguard company assets and property against unauthorized use or disposition.
- The Company assets include but are not limited to physical property, intellectual property, patents, trade secrets, copyrights, and trademarks.
- Additionally, it is the responsibility of company line management to ensure that staff is aware of, and fully complies with the company's security guidelines, and all relevant laws and regulations.

Compliance

- Management is responsible for conducting periodic reviews and audits to assure compliance with all policies, procedures, practices, standards, and guidelines.
- Employees who fail to comply with the policies will be treated as being in violation of the Employee Standards of Conduct and will be subject to appropriate corrective action.

Figure 6.3 Sample physical security policy.

Procedures should also include logging procedures that allow for all events—not just events requiring responses—to be logged for audit purposes or for purposes of follow-up (Figure 6.3).

Summary

The nature of physical security for a data center should be one of concentric rings of defense—with requirements for entry getting more difficult the closer we get to the center of the rings. The reason for this is obvious—if we take a number of precautions to protect information accessed at devices throughout the organization, then we must at least make sure that no damage or tampering can happen to the hardware on which the information is stored and processed. Having said that, the principle of consistency must still be applied. There is no point in building physical access controls at a cost of several million dollars if the potential damage that could be done to a data center is less than several tens of millions of dollars.

Chapter 7

Disaster Recovery and Business Continuity Planning

Kevin McLaughlin

Contents

> There must be a self-regulatory process…with internal rules, as that is efficient. However, self-regulation is not enough—you need both legislation and self-regulation.
>
> **—Bernhard Otupal**
> *Interpol*

Introduction

Organizations continue to take large-scale losses and even go out of business by not adequately planning for large-scale disasters that affect their ability to conduct business. When a disaster hits an area, its socioeconomic effects are compounded when the citizens of that area also end up out of work and not receiving a paycheck. These citizens often file civil lawsuits for damages. These lawsuits frequently cite management neglect and lack of disaster recovery (DR) planning as one of the reasons for seeking damages. Lawsuits like this often add to the postdisaster economic distress suffered by communities and businesses. Picou et al. (2004) stress that the negative effects of a disaster can damage communities and their citizens for a long time after the event. These communities struggle through postdisaster recovery and have a hard time being successful with their postdisaster recovery efforts. One of the most negatively impactful activities that slow down the recovery process is excessive postdisaster litigation. Although many items contribute to this slow recovery, Picou et al. (2004) contend that "none are as debilitating as the litigation processes that… ensue to redress" (p. 1494) the negative socioeconomic effect experienced by the members of the community.

Due to the heinous socioeconomic effect a disaster can bring to both an organization and the community within a geographical region when its businesses are unprepared to recover from such an event, it is important to have necessary business continuity and DR plans in place.

Background

Many organizations voluntarily spend money and time attempting to design DR systems, processes, and methodologies that will enable them to continue business operations in the event of a disaster. To bring the appropriate systems up, it is important that organizations are able to contact the resources needed and that they have methods in place to ensure that resources can actually make it to the recovery area. Adding strong leadership roles for the responding resources is also of critical importance for successful DR postevent recovery (Biddinger 2007). Another necessary component of successful recovery is ensuring that information technology professionals spend time testing the hardware and equipment needed to make sure the organization can recover business critical systems in the time required as cited by the senior management. Before an event, organizations need to complete a business impact analysis (BIA) so that they clearly understand which systems need to be restored to maintain adequate enough business operations.

There is currently a dearth of government regulation that requires business entities to have robust business continuity and DR plans, strategies, and infrastructure in place. Lacking this regulation, organizations need to look elsewhere to determine how to plan, implement, test, and assess business continuity and DR plans. Thankfully, there are, however, many standards in place that assist organizations in designing effective business continuity and DR plans. The National Institute of Standards in Technology (NIST) Special Publication (SP) 800-34 is one such standard and its book on contingency planning outlines methodologies for organizations to follow and strongly suggest that each organization have such plans in place so that they do not suffer unrecoverable postdisaster loss.

In order to have an effective DR program an effective DR process framework needs to be developed within the organization. This process framework allows an organization to put a sustainable, repeatable and easy to follow step by step process in place for handling the management of their DR solution. While at the University we used the following: Design and approve the DR Policy, Conduct and Complete an organizational BIA, Develop and get buy in for the recovery strategy as focused on the BIA results, Design the organizationally approved DR plan, Plan and Complete training and testing, and lastly make sure that the plan is a living document that is maintained ongoing throughout the year.

Tulane University, like many organizations in New Orleans, was prepared for an event like Katrina but it did not have plans on how to recover from such an event and ended up missing its August payroll run, an event that compounded the trauma that many families were already going through (Anthes 2008). John Lawson, Vice President and Chief Information Officer (CIO) for Tulane, stated that

> We did have to face the music. We stopped paying adjuncts on August 29. We stopped paying part-time faculty and staff members on September 30. Beginning November 1, we began using vacation and sick leave to help pay full-time faculty and staff members (The Chronicle of Higher Education 2005, p. B.203).

The aftermath of the Katrina disaster was tough on the communities affected and better business continuity and DR planning would have gone a long way toward minimizing the socioeconomic downfall that the event brought to New Orleans and its surrounding communities. It took so long for universities in Louisiana and Missouri to recover from the aftermath of Katrina that 26,000 students in the state of Louisiana and 9,000 students in the state of Mississippi failed to return to their schools (Marcus 2007). Two years after the event, the University of New Orleans was still 6,000 students under its pre-Katrina enrollment numbers and Loyola University was still 1,000 students under its pre-Katrina enrollment numbers. A secondary effect of this decrease in enrollment is that 217 faculty members who lived and worked in the New Orleans community were fired from their University positions (Marcus 2007). This means that postdisaster within their local institutions of higher education, the community of New Orleans had 7,217 fewer consumers' spending money and helping their community rebuild and recover its economy. In a separate disaster event, the United States 9/11 Twin Towers attack, it was noted that for a number of months after the event, workers in New York City experienced a decrease in the number of hours at work. This decrease rebounded within a 6-month period, but it does confirm that a community does suffer negative postevent economic effects (Hotchkiss and Pavlova 2004).

One of the major issues faced by organizations when they are considering business continuity and DR strategies such as integrated automation to facilitate business continuity process management (BCPM) and DR high availability (Lumpp et al. 2008) is the large budget that is necessary to implement a successful business continuity and DR program. These monies are often needed on an annual basis and they are to be spent on contingency items that might never be used. In 2009, a lot of IT shops were facing budget shortfalls, with capital budgets being nonexistent in many organizations. With the current economic woes, it is not uncommon for senior executives to view redundant infrastructures as cost-doubling effort wastebaskets that they are dropping money into but that has zero practical and likely no future use or benefit (Rice 2009). It is very difficult for managers within an organization to spend scarce dollars for an event that might never occur.

> Tulane did not have a formal DR plan for replacement of machines with any outside vendor or institution. That was a cabinet-level decision, made during times of fiscal stress. We had just shifted to a decentralized system for fiscal management, so IT was a shared resource. When I presented the plan for off-site DR, it was for $300,000 a year or so. We decided that we could not ask the deans to pay for that as they were already upset about recent budget cuts and increased IT recharge rates. (The Chronicle of Higher Education 2005, p. B.201)

Of interest to note is that John Lawson, the CIO of Tulane, has related publicly that after Katrina, his off-site DR plan was approved at a cost of approximately $600,000 per year, double the amount Tulane management turned down before Katrina.

Senior managers for organizations need to understand that the infusion of technology across their business processes makes ignoring business continuity and DR planning borderline gross neglect (McKinney 2009). In many cases, the failure to follow all of the seven NIST SP 800-34 contingency planning steps to fully prepare for a disaster can be seen as a failure of the organization's senior management and lead to a civil lawsuit for damages. In some cases, this lack of prudence by organizational management can compound events subsequent to a disaster to such an extent that the organization is incapable of postevent recovery. In some postevent cases, we can even go as far as to say that "managerial errors are the root causes of the technological disasters" (Shaluf 2007, p. 387).

Developing the Contingency Policy

One of first items that information assurance/security professionals need to do to ensure that their organization is going to take the necessary precautions to make sure that if a disaster occurs they will be ready and prepared to recover is to develop a Business Continuity Contingency Policy. As is true with any policy, vetting and alignment with organizational senior management is the first thing that needs to take place. Once this approval of the policy takes place, it then needs to proceed through an organizational governance process to ensure that proper buy-in from the affected community members' takes place. The activities during this time will be ongoing review, edit, review, and finally acceptance and alignment. The vetting of organizational policies should also make sure to include review by the organization's general counsel. When finalizing the policy, keep in mind that 100% alignment is not usually possible and the organizational governance process should take that into account.

Business Impact Analysis

A discussion on BIA and a sample procedure are included in Appendix B.

Controls and Mitigation

Bergland and Pedersen (1997), in a report on the effects of safety regulation on the safety and well-being of Norwegian fisherman, found that costly regulation induced "the individual rational fisherman to behave in a way which increases their risks" of injury (p. 291). This behavior is caused by a fundamental risk analysis being conducted on the part of the regulated entity. Will it cost me more to follow the regulation than it will to suffer the accident or loss caused by a negative event? Extrapolating that risk analysis to the area of business continuity and DR planning, it is feasible to believe that senior business managers in other industries will conduct similar analyses. Will it cost me more to implement the required business continuity and DR infrastructure than it would for me to recover from a catastrophic event that may or may not occur sometime in the future? This is an impactful question that needs to be fully considered in our current economy downtrend that is causing organizations to pull back from IT spending and is in line with the current economic trends, which depict IT budgets trending downward instead of upward (IndustryWeek 2008).

Government Involvement in Business Continuity and Disaster Recovery

The goal is not to eliminate the risk but to design business continuity and DR strategies that generate more benefits to the community than the negative effect of the costs incurred (Viscusi and Gayer 2002). This type of cost–benefit analysis and risk- versus cost-based thinking is a critical component to consider when deciding if business continuity and DR strategies should be implemented.

Facilitated Business Continuity and Disaster Recovery Theory

One scalable and relatively easy way to make sure that all of your business IT departments have a successful DR plan is to leverage the understanding and capabilities of the Facilitated Risk Analysis and Assessment Process (FRAAP) and create your DR teams and methodologies in the same manner as the FRAAP. This includes splitting the workup among the teams, making sure each team has one trained DR specialist/trainer who is responsible for instructing department DR personnel on how to make use of the templates and tools associated with the organization's DR efforts.

Conclusion

> My children will live with the mistakes I make.
>
> **—Representative Zoe Lofgren**
> *in a speech on government regulation of DR methods for the Internet*

Lawsuits are also not the answer to resolving the issue of successful postdisaster recovery, and are actually counterproductive to the goal of maintaining a stable socioeconomic climate that is ripe for successful recovery (Picou et al. 2004). Many of the businesses that suffer a disaster do not have the financial means to recover and continue their operations in the community, and having to pay postdisaster settlement costs will drive them closer toward bankruptcy and not being able to reestablish normal business operations.

Because the CIO of an organization has a fiduciary responsibility to protect corporate assets in good times and bad times (Lumpp et al. 2008), business continuity and DR planning is the component that has to be put in place if organizations are to remain open and viable after a disaster strikes their geographical region. "Data recovery is now a $20 billion per year sector of IT" (Preimesberger 2008, p. 31), which is a strong indicator that the increasing number of natural and man-made disasters that have hit communities and the publicity generated over those events, which discuss how many businesses failed to recover, is finally causing organizations to start implementation of recovery plans, tools, and strategies. A lot of organizations have changed their posture and thought process in regards to BCP and DR planning and have decided to make efforts in this space a part of Organizational strategic planning instead of just nice to haves (Payne 2010). A plethora of DR software and hardware are available to IT managers; tools like Ecora, Orange Parachute, Compellent, NetApp, Xiotech, SunGuard, open source DR software from Berkeley, etc. (Preimesberger 2008), allow organizational IT shops to create recovery plans and methodologies. Organizations are starting to understand that developing and maintaining a comprehensive business continuity and DR plan and supporting infrastructure is of critical importance (McKinney 2009). The Loews Corporation, a New York–based holding company, in part because of the 9/11 disaster, has developed multiple points of redundancy and recovery plans just in case they are affected by future events (Mearian 2003). Similarly, the ninth item on the list of the top 10 trends in higher education is to increase focus on planning for catastrophe and DR (Martin and Samels 2007).

There are many areas that the government can be involved in when it comes to protecting the United States' infrastructure and improving DR among government and private organizations. One of these items is to assist in the development of standards, best practices, and training (Anonymous 2009). Good examples of the type of standards and best practices that governments can develop and promote are the US Government's NIST 800-34 Contingency Planning and the UK Government's ITIL Continuity Planning.

A combination of government regulation, self-regulation, government and private training of business continuity/DR professionals, and government and private sector partnerships and associations is necessary to minimize the negative socioeconomic effect caused by a large-scale disaster. The partnership programs should be modeled after the Federal Emergency Management Agency's (FEMA) free post-9/11 integrated government and private sector training for emergency responders across the United States (Whitworth 2006). The business continuity/DR integrated training courses should consist of free nationwide awareness classes on why businesses need to be worried about and prepared for a disaster affecting their ability to conduct business and the economic effect suffered by their community when they fail to go back into business after a disaster. Additional courses should be offered to business and IT management on the seven NIST 800-34 contingency and ITIL continuity planning steps.

References

Anonymous. (2009). Self-regulation plans polarise industry. *The Safety and Health Practioner* 27(12), 8.

Anthes, G. (2008). Tulane University; following Katrina, the university's top priority was getting its people paid. Now its payroll system is safer than ever. *ComputerWorld*, *Special Edition* 1–2.

Bergland, H., and Pedersen, P.A. (1997). Catch regulation and accident risk: The moral hazard of fisheries' management. *Marine Resource Economics* 12, 281–291.

Biddinger, N. (2007). The information technology role in DR and business continuity. *Government Finance Review* 23(6), 54–56.

The Chronicle of Higher Education. (2005). A look back at a disaster plan: What went wrong and right. *The Chronicle of Higher Education* 52(16), B200–B203.

Hotchkiss, J.L., and Pavlova, O. (2004). The impact of 9/11 on hours of work in the United States. *Working Paper Federal Reserve Bank of Atlanta* 16.

IndustryWeek (2008, November). Capital budgets for IT hit the wall. *Information Technology* 68.

Lumpp, T., Schneider, J., Holtz, J., Mueller, M., Lenz, N., Biazetti, A. et al. (2008). From high availability and DR to business continuity solutions. *Systems Journal* 47(4), 605–619.

Marcus, J. (2007, October 5). Katrina-hit campuses try to return to normal. *Times Higher Education* 1–2.

Martin, J., and Samels, J. (2007). 10 trends to watch in campus technology. *The Chronicle of Higher Education* 53(18), B.7.

McKinney, M. (2009). Plan before panic. *Hospitals and Health Networks* 83(11), 35–38.

Mearian, L. (2003). Global firms confident about DR. *Computerworld* 37(12), 6.

Payne, L. (2010, January). Changing security theory to security practice. *Security Magazine* 60–63.

Picou, J.S., Marshall, B.K., and Gill, D.A. (2004). Disaster, litigation and the corrosive community. *The University of North Carolina Press: Social Forces* 82(4), 1493–1522.

Preimesberger, C. (2008, July 21). On the brink of disaster. *eWeek* 31–38.

Rice, J. (2009). Budget ax falls on DR. *Computerworld* 43(2), 28.

Shaluf, I.M. (2007). An overview on the technological disasters. *DPM* 16(3), 380–390.

Viscusi, W., and Gayer, T. (2002). Safety at any price? *Regulation* 25(3), 54–63.

Whitworth, P.M. (2006). Continuity of operation plans: Maintaining essential agency functions when disaster strikes. *Journal of Park and Recreation Administration* 24(4), 40–63.

Chapter 8

Continuity of Operations Planning

Jeffery Sauntry

Contents

Americans can always be counted on to do the right thing…after they have exhausted all other possibilities.

—Sir Winston Leonard Spencer Churchill
(November 30, 1874–January 24, 1965)
British politician and statesman known for his leadership of the United Kingdom during World War II and the first person granted honorary citizenship of the United States

Introduction

Continuity of operations planning (CoOP) is an important core capability that every business needs, but few even attempt to do well, much less write down, implement, or actually test under real-world scenarios. Many organizations have never seriously considered the topic because it could be too complex, might cost some money, might not help them hit this quarter's revenue target, and with a similar scorn they have for most forms of insurance, they may never even need it. For some reason, as Sir Winston Churchill suggests, most organizations will try almost everything else before actually putting a viable, complete, fully implemented, and tested CoOP in place. Government and industry regulations are major drivers that have forced some organizations to begin tackling the topic by requiring the establishment, testing, and proof of ongoing maintenance to demonstrate compliance or lose certain industry certifications. There are still too many corporations, government agencies, and small businesses that could realize tremendous benefits by implementing even limited continuity of operations plans. CoOP may not always be lead by information technology (IT) security professionals, but a thorough understanding of the topic, how security requirements can be integrated into the plans, and mastering the industry's best practices associated with creating a CoOP strategy should be a core competency of every member of a security organization.

Background

As a security professional, you may be asked to lead or participate in the CoOP process. A key consideration for most CoOPs is the requirement that the safeguards and standards of confidentiality, integrity, and availability be maintained even when operating during a disaster. It seems a very logical requirement, but one that becomes increasingly difficult to achieve when an organization has to relocate key processes to another facility. Factors such as having multiple tenants (e.g., some of your fiercest competitors could be co-located in the same recovery facility) and "easy everyday" tasks are hobbled by the lack of supporting infrastructure and poor planning that is all too common during a disaster. According to Abraham Maslow's hierarchy of human needs, tier one needs are water, air, food, and sleep, closely followed by the second tier of "security needs," which includes steady employment, good health, and shelter from the environment. There is a reason that food, water, and sanitation are part of the first supplies shipped in by first-responders after a natural disaster and not computer cables and pallets of high-capacity storage devices. Consider how hard it would be to secure simple items to recover your operating environment if you didn't have the tier one items available, much less the items you would need to recover your daily operations (e.g., electrical power, media, and backup copies of data files) if you didn't start to think about them until after a natural disaster had occurred? The upside is that the process is straightforward and huge strides can be made to make your organization more resilient with even modest efforts to plan for outages and disruptions before they happen.

There are some emerging business trends that make continuity of operations much more practical than ever before. The globalization of many organizations can be leveraged by spreading business capabilities across multiple, geographically dispersed locations to minimize the effect of losing access to a single facility in an area affected by a local event. Telecommuting and other unified communication trends can be harnessed to leverage a broad pool of personnel that can remain in constant communication with one another even if the organization's infrastructure is damaged or rendered inoperable by utilizing secure communication channels across public networks that may still be available during a disaster. Finally, virtualization can have a dramatic impact on the speed of recovery if properly leveraged. It will redefine how decades of IT security professionals have defined a "standby site" that can very literally be enabled with a few simple procedures versus large-scale logistical efforts that involve hours or days of acquiring and assembling hardware followed by man-days of installing operating systems, applications, and applying patches before even the first attempt could be made to restore data that may have been stored hours away in a separate physical facility. Virtualization, cloud computing, and robust telecommunication provide new capabilities as part of CoOP that can assist organizations in achieving the security, availability, and confidentiality requirements of the new "always on" business model with limited or no interruption even during disruptive events.

Patience, Persistence, and Overcoming Organizational Resistance

There are good reasons to have a well-rehearsed and complete CoOP. Unfortunately, there seems to be a never-ending list of excuses that most organizations turn to in order to explain why they can't master a program that can literally be the difference between keeping the doors open after a disaster or closing down operations forever. Understanding and anticipating the obstacles and objections will be critical to getting your organization's program off the ground. The excuses take many forms and stem from long-standing personal, organizational, and institutional mind-sets. Senior managers to rank-and-file staff members will protest from participating and procrastinate when asked to contribute because a disaster hasn't affected them before in their long and illustrious career. Despite the common adage that "hope is not a strategy," these fine coworkers (aka ostriches with their heads in the sand) are content to gamble that it won't happen "on their watch." Besides, like most political kamikazes in any organization, by the mere act of proactively asking them about the topic or soliciting their participation in the planning process, it is clear that the big red bull's-eye has obviously been placed on your back by someone in authority.

If a plan is needed, obviously, you will be the de facto scapegoat if it doesn't work. You might want to remind them of some of the statistics found later in this chapter and in Chapter 7 of this book, which they can ponder on in the unemployment orientation meeting surrounded by an ocean of their peers with similar skill sets who will soon be competing with them for jobs in a small geographic area they call home, which will probably soon be reeling from the economic devastation that is common after major disasters. Ironically, the organizations that did have a good CoOP in place may be the only ones still hiring because they have achieved the ultimate goal of any good CoOP or business continuity planning (BCP)—they are still in business.

Consider as well how to best overcome resistance and skepticism generated as part of the organization's corporate culture or individual personal agendas. Many employees and departments tie a close association between the limited knowledge of their internal operations and the value they bring to the organization. Right or wrong, many employees feel their job security may be threatened if someone other than themselves knows *exactly* how a business process works because everyone knows "the show can't go on without the star; coal stoker in the boiler room keeps the fires burning; it's the locomotive that pulls the rest of the train, etc." Simply explain that the senior management team *has* recognized that their role and function is so important it has been *selected* to participate in this important program, so that in the unfortunate event that a tragedy does happen, "the show" will go on. For even the most resistant participant, this approach normally works, especially when they consider the alternative of not being included in a program that is attempting to identify the core capabilities needed to keep the organization afloat. If it still doesn't work, look for another employee with similar knowledge or go back to your executive sponsor to discuss alternative "motivational techniques."

Uncooperative individuals will not be your only challenge in the early stages of developing the CoOP. Considerable amounts of the institutional knowledge you need to build out the plan may exist but may not be in a very useful or reusable format. With the exception of some government agencies or U.S. Department of Defense contractors, consider how much effort and organizational discipline it takes to document and capture the daily workflows that are required to keep an organization running smoothly. Many employees may know how to do their job or a specific task, but rarely will it be captured in a usable format that you can leverage to understand the key aspects of a business process, the risk associated with specific elements much less support any cause and effect analysis a disaster may have on it. The upside is that if a picture is worth a thousand words, a good Visio or Unified Modeling Language (UML) diagram will seem invaluable at this point if you are willing to invest the time to extract and capture this very important knowledge. Leverage the power of visual references to facilitate the conversation, map key dependencies, and talk about risk and threats to the business process with key stakeholders early in the planning phases. Not only will you gain credibility and cooperation with someone you may call on later to help support your protection recommendations, but these diagrams will also be very valuable to you later when you need to establish other key CoOP artifacts such as use cases, testing scenarios, risk/probability ratings for specific threats, etc. Patience, persistence, strong written and verbal communication skills, and documenting complex tasks to a fine level of detail will require core competencies that you must demonstrate throughout the entire process. This time and effort investment will pay huge dividends to you professionally well beyond the scope of the CoOP project. Your value to the organization will increase dramatically as you demonstrate to senior management your new, deeper understanding of how the business works, which will provide you valuable insight on how to best protect it. It is this knowledge and application of your technical expertise that will have the greatest effect on your career.

Critical Success Factor—As you begin to develop the plan and solicit input from other staff members, set a good example by stressing the importance of maintaining the confidentiality of the plan. Assuring people that their input and the detailed knowledge of business operations will be properly safeguarded throughout the life cycle of the program will promote a degree of trust between parties and should improve collaboration efforts. Properly mark the CoOP and supporting documents with an appropriate data classification and corresponding limited distribution disclaimers. Once the plan is complete, it should only be shared with employees or partners on a need to know basis, which is bound by current and binding nondisclosure agreements (NDA).

Purpose and Scoping of CoOP

Determining and being able to articulate the purpose of the program is the first step of the planning process. Given the level of effort, staff involvement, and possible expense associated with developing the program, it is typically sponsored by a senior member of the management team or the business owner. It is important to understand *what* and *whom* they expect to be included in the planning process. In many cases, it is useful to gain insight into the motivation and timing associated with implementing the CoOP program. There could be a particular risk that they feel is threatening the business, a requirement related to a contractual or regulatory requirement, or it has become necessary to support a strategic growth initiative (e.g., mergers and acquisitions, raising capital, divestitures).

Expect that the initial scope of the plan will typically be described in broad or abstract terms (e.g., patient electronic medical record or e-Commerce site) or general business functions/processes [e.g., accounts receivable, build-to-buy process, enterprise resource planning (ERP) system, or new customer acquisition]. At this point, don't worry about all the components in the supporting technical infrastructure, but try to verify if there are any specific risks or threats they are particularly concerned about so you can incorporate them into your final plan for discussion with the other members of the team. Attempt to identify if there are any targeted windows for recovery or tolerable outage periods that should be incorporated into the plans' objectives. It is very important to be able to capture and articulate the scope, goals, and objectives when you are discussing it with others. By properly framing the conversation and including or excluding certain business processes, you will be able to focus your plan development efforts more effectively. Don't try to boil the ocean and take on too much (e.g., 100 business processes, 10 facilities, the entire IT infrastructure) on the initial version of your plan. You want the plan to be ambitious and complete, but it can quickly die under its own weight and complexity if not properly limited in size and scope. Once you have the plan completely implemented for a few business processes, it is easy to expand and adapt to others.

Critical Success Factor—The visibility of executive management support during the planning process will often mean the difference between your success or failure. Suggest to your executive sponsor that *you* craft some e-mail message content summarizing the program, objectives that clearly set the expectation that key stakeholders' *active participation* is expected in the coming weeks. Ask that your sponsor send the message to each of the critical team members that are expected to participate in the CoOP process to jumpstart the program, establish it as a high-priority project with senior executive visibility, and it will get you off on the right foot with the other members of the team.

Example of a Purpose Description (IT and Web-Centric CoOP)

This disaster recovery (DR)/CoOP provides the required instructions to support contingency operations for disruptions to the <business function(s)> of <company XYZ's> <geographic location> operations. This plan addresses events and declared incidents that could disrupt the network, communications, and ability to generate revenue through critical online assets and retail store operations across the organization. It contains operational procedures to address limited service interruptions, <business function(s)> outages, and situations that could threaten the security of the communication and application infrastructure.

<Company XYZ> is prepared to respond to a wide range of events, emergencies or threats that may disrupt operations. Emergencies are any unplanned events that can potentially cause death or significant injuries to employees, customers, or the public; that can shut down an organization, disrupt operations, cause physical or environmental damage, or harm the organization's public image. Government-declared emergencies run the gamut from fire, hazmat incidents, weather-related incidents, terrorist activity, cosmic/radiological incidents, civil disturbances,

or human illness pathogens and often limit employees' physical access to the <Company XYZ's> <geographic location> operations or facilities. IT or cyber-related threats to the <Company XYZ's> production environment can affect the confidentiality, availability, or integrity of the Internet-facing assets that are used to generate revenue for the organization. Technology-centric threats range from malicious code, hacking, intellectual property theft, and phishing attacks that can result in data loss or compromise adherence to industry and government compliance regulations.

<Company XYZ's> CoOP is designed to optimize the response of the organization by quickly identifying and responding to any of these threats quickly and methodically. The response capabilities of the organization have been developed to provide a robust operational capability that is not dependent on a single facility or in the case of the supporting IT infrastructure, a single critical device or point of failure. The probability (likelihood that an incident will occur), frequency (how often an incident occurs), and the severity (effect of an incident) are factors that weigh heavily into the DR/CoOP process. Those events that could disrupt operations are evaluated based on criticality and probability.

The (Executive or Committee) has identified the assets supporting the revenue-generating, new customer subscription and bill-paying capabilities as critical business services requiring a dedicated DR/CoOP. The main purpose is to ensure that <Company XYZ> is able to communicate and operate both during normal operation and during a state of emergency with customers, subscription services, credit card processing partners, and employees.

Because the <Company XYZ's> web presence is reliant on a combination of company-owned assets and leased services, this document sets forth the requirements to maintain the continuity of the network, revenue-supporting applications, and associated mission-critical IT services necessary to keep the organization economically viable during disruptive events.

Specific DR/CoOP objectives and recovery goals:

1. To provide for the protection of lives, property, network and information assets supporting the <Company XYZ's> Internet-facing sites, and supporting infrastructure from outages caused by natural and man-made disasters or digitally enabled (cyber) threats.
2. To enable orderly and timely migration from primary to secondary data center resources as necessary to support revenue-generating portions of the organization within a 4-hour response window.
3. To provide for quick continuation of essential network functions supporting the <Company XYZ's> web site under emergency conditions in a disciplined response to the aftermath of a disaster.
4. To provide procedures and provisions for the utilization of alternate facilities as needed to continue essential support functions.

5. To provide procedures to be followed in preparation for or in response to the aftermath of an emergency.
6. To return the <Company XYZ's> web presence or support to normal operations as quickly as possible after an emergency or declared event.

Conducting Business Impact Analysis and Creating Workflow Diagrams

There are a wide range of techniques you can utilize to conduct a business impact analysis (BIA). Most follow a basic format to evaluate a wide range of threats against assets or processed deemed "in scope" for the CoOP. Most will require an evaluation of the adverse effect expressed as either a qualitative (e.g., educated guess) or quantitative (e.g., numerical value or financial effect) value. As mentioned in the previous example, purpose description, keeping the categories, and threat vectors generic is sufficient for most planning purposes, but not for each organization or some compliance requirements.

Adapting the BIA to meet the needs of the organization, audience, and regulators should dictate which type of BIA you conduct. If the organization's decisions relies on hard and accurate cost figures, then using a technique that utilizes specific threats against a discrete number of critical business assets that relies on historical occurrences or threats with a high probability that can express the results of damage or negative effects in terms or lost revenue or recovery cost may be the best approach. Many organizations may not have the level of granular cost detail to make these computations possible. If that is the case, then establish this fact early with the executive sponsor, or use a BIA technique that will provide an appropriate level of detail to support planning purposes and any associated expenditures to protect critical assets. In other instances, there could be very specific requirements associated with how a BIA needs to be structured to meet regulatory or business requirements. For example, in businesses that utilize credit cards, there are specific standards and practices that must be adhered to as part of Payment Card Industry–Data Security Standard (PCI-DSS), which lists specific threats and protection techniques that are required to achieve certain levels of compliance that are required if a business wants to continue accepting credit cards for purchase payments.

Certain departments will help identify the risks and circumstances that need to be addressed under specific conditions that may need to be considered as part of your planning. Legal departments may need the CoOP to address circumstances such as "litigation hold" or record retention requirements that have to be maintained even when an emergency has been declared and data processing has been moved to an alternate facility. Many business models, especially in service industries, rely on a complex set of third-party service providers and the availability of these processes needs to be considered as an integral component of your plan. Business partners that provide critical services such as off-site storage of backup media, web hosting and content delivery providers, telecommunication, utility, property management, and credit card processing companies, or supplier/partners/distributors with ERP systems integrated into your companies' daily operations will need to be taken into consideration when assessing the "impact" of some risk factors as part of your BIA. The bottom line is that there is probably a *best* way to conduct a BIA for your organization, but make sure you adapt your approach to produce useful artifacts that will be readily accepted by the senior management and other members of the CoOP team.

The ITIL framework has a very good baseline processes for conducting a BIA as part of IT Service Continuity Management or via a risk management approach using the techniques found in the Management of Risk (MOR) series of publications. Make a quick search of the publicly available templates via government-sponsored sites as well those that include publications by NIST (e.g., 800 series), Software Engineering Institute's CERT program, state and local government sites or many universities' sites, which have great templates that you can quickly adapt to your organization's needs.

Another common challenge associated with developing a credible BIA is identifying sources of current threats, trends, and associated costs with losses or data breaches. Keeping the content simple and relevant is crucial when tapping into industry reports. Start with simple threat criteria such as geographic location, industry-specific data, and then establish broad categories to compartmentalize the information you find that may be relevant to your organization or specific threats. Categories such as physical, IT/cyber, regulatory, and business process threats are a good starting place when gathering data about threats.

There isn't a definitive, single place wherein everything is neatly packaged to fit in these categories. Use these suggestions as representative examples in addition to trade associations, professional certification groups, and government web sites to start building your CoOP content.

For a listing of natural disasters (in the United States) that could result in the loss of physical assets or entire facilities, start with this site populated by agencies such as FEMA for the areas in which your organization operates (http://www.fema.gov/news/disasters.fema).

Some state, county, or local governments provide even more detailed information that may be useful for your planning purposes. Many will be affiliated with professional associations such as the State Emergency Response Team (SERT) or regional associations. A good example is the Florida Business Disaster Survival Kit, sponsored by the Tampa Bay Regional Planning Council (http://www.fldisasterkit.com/index.shtml).

IT and cyber threat sources are a broad topic that has many sources that could be updated almost daily. Broad categories and annual trends that are expressed in layman's terms will be most useful for planning purposes. Avoid being too technical, there are more appropriate places in the CoOP for items such as architecture diagrams and OSI threat models, which we will explore later in the chapter. Some of the most respected annual reports related to IT and cyber threats and fraud-related crimes include

- Computer Security Institute/FBI *"Annual Crime and Security Survey"* (www.gocsi.com)
- Ponemon Institute "*20xx Annual Study: Cost of Data Breach*" (www.ponemon.org)
- Verizon Business *"20xx Data Breach Investigation Report"* (www.verizonbusiness.com/resources/reports)
- Certified Fraud Examiner "*20xx Report to the Nations on Occupational Fraud and Abuse*" (http://www.acfe.com)

An example of industry-specific publications that cover industry trends and regulatory compliance–related issues include examples from the information Security Media Group (iSMG) targeting banking, Government, and health care verticals (http://www.ismgcorp.com/research.php).

Many other examples exist from groups such as analysts, vendors, and trade associations, but remember to bring an objective and skeptical mind-set depending on the source and sponsors of any third-party publication.

For the category of business threats, consider the external third parties that your organization relies on for critical services or for products to support key business functions. Also, consider the risks that could be introduced by the connections to either suppliers or, in many cases, your customers into your computing environment or supply chain. There is no universal template or single web site for finding info on these threat vectors, but for each third party service, consider scenarios that could affect the confidentiality, integrity, or availability of your organization. It can be helpful to consider a simple supply chain workflow that describes how goods, information, or services are produced, stored, packaged, sold, paid for, and ultimately, delivered in order to get started. Ask someone in the respective department about their workflow or business models, which includes third-party services, and you're likely to hear phrases like "cash to order" from the accounting team or "build to buy" or "source to sell" from someone familiar with internal operations who understands the inner workflow of the organization's ERP system. Carefully document these business processes, looking for opportunities to identify supporting processes, IT infrastructure connections, and application dependencies to external third parties.

Consider the workflow and interdependencies of the following business functions required to enable a basic business to consumer (BtoC, or B2C) e-Commerce site. High-level business functions such as marketing, sales, production of the electronic content or physical goods, inventory management and distribution, and payment may be as simple as a single web server hosted in a single facility. More likely, it crosses multiple facilities, employees, departments, and partners to run efficiently.

Consider the following departments and business functions to get your workflows diagrams started. Not each will be represented in every model or workflow, but it will serve as a broad topic list to consider when meeting with key stakeholders. Common business functions and departments include: Accounting, Accounts Payable, Advertisers, Accounts Receivable, Bank Credit Card Processing, Board of Directors, Business Partners, Content Providers, Copy and Marketing Materials Center, Customers, Customer Service, Design, End Users, Engineering, Executive Management Team, Facilities, Hosting and Managed Service Providers, Human Resources, Information Services (e.g., Database, Network Infrastructure, Security, Change Control, Help desk), International Divisions, Inventory, Legal Department, Mail Service, Manufacturing, Marketing, Motor Pool/Transportation, Packaging, Payroll, Publications, Purchasing, Quality Assurance, Receiving, Reception, Research and Development, Sales, Physical Security, Shipping, Suppliers, Telecomm, Utilities, and Warehousing.

Critical Success Factor—Always send a copy of your completed diagrams or workflows back to the original source of the information for verification of accuracy and completeness. They will appreciate the follow-up and often provide feedback or updates based on knowledge only they could provide about missing items or interdependencies you may not have been privy to as an external observer.

Documenting a Functional Overview of the Current Environment

High-Level Narrative

As the early stages of a CoOP come together, a high-level narrative that describes the business processes, critical services, or departmental priorities should be completed. Too often, a CoOP team builds on legacy documentation that relies heavily on institutional knowledge to add context and understanding to cryptic system architectures or generic workflow diagrams. Once the scope and operating environment have been established, use the narrative to explain the main components, services, and business processes supported. This section will be particularly valuable to nontechnical or supporting staff that may have been a part of the workflow but may have never known how the components interrelated. By developing a simple diagram to accompany this description, establishing an orientation for new members of the CoOP team will be streamlined. It should be clear in the narrative that services, infrastructure, and partner connectivity will need to be incorporated into the CoOP if this business capability is expected to function effectively during a disruptive event. Internet service providers (ISP), telecommunications, networks, and detailed inventory and configuration documentation can be added here, often embedded as artifacts within the plan, or listed as appendixes to add technical depth to the narrative and diagram.

Example of High-Level Narrative and Supporting Diagram

The diagram on the following pages represent the connectivity and core computing environment to support the <Company ABC's> online presence. The core applications are supported across three operating systems (Windows, Red Hat Linux, and Solaris). Most applications rely on an instance of Oracle to manage and maintain databases used to service customers, retail centers, or to serve web content. This Oracle instance is utilizing Data Guard to increase reliability and uptime and will be used to keep the data sets between primary and secondary facilities in sync. Ongoing management of the IT environment is accomplished using <Product A>, <Product B>, and <Product C> for activities such as application version control, patching and source code integrity verification to assist with governance and compliance mandates. Core IT services required to establish and maintain the <Company XYZ's> web presence and security include domain name service (DNS), Microsoft's Active Directory (AD) for user and resource provisioning, and Virtual Private Network (VPN) for secure remote connectivity. Brick and mortar franchise facilities (aka retail stores) connect via IP-Sec VPN connections using preshared secret keys. These remote sites require connectivity to key applications hosted in the <primary data center city> facility to accomplish critical tasks such as managing inventory, capturing customer metrics, and posting credit card transactions via the on-site POS terminals.

Strategic partners for the <Company XYZ> operations include

CreditCard ABC—credit card processing and payments
Reach Everyone PDQ—marketing services
Electro Cash DEF—payments
SuperWamo WebFarm—content distribution and acceleration

IT security mechanism include <security vendor of choice> malware (e.g., virus, worms, malicious code) protection, and intrusion detection systems (IDS) to address threats such as denial-of-service attacks (DoS) and other network-based threats. Firewalls are used to further segment the network from Internet traffic.

Contracts are currently in place with three vendors to provide support services for the BCP/CoOP. <Telco PDQ> is the primary vendor that provides a hot site facility in <secondary city> in the event that production has to be moved out of the <primary data center city> facility. The <primary data center city><Company ABC's> production environment is hosted in a managed <managed services provider> facility that has inherent capabilities to address short-term threats (e.g., limited duration power outages).

Additionally, <BCP Contractor X> is under contract to provide cold site services for a limited number of applications at an alternate processing facility. This site would require many hours, if not days, to become fully operational to support the cold site applications. <Media pick up and storage company MNLOP> is providing record and media retention services to support secondary facility relocation requiring access to backup media (Figure 8.1).

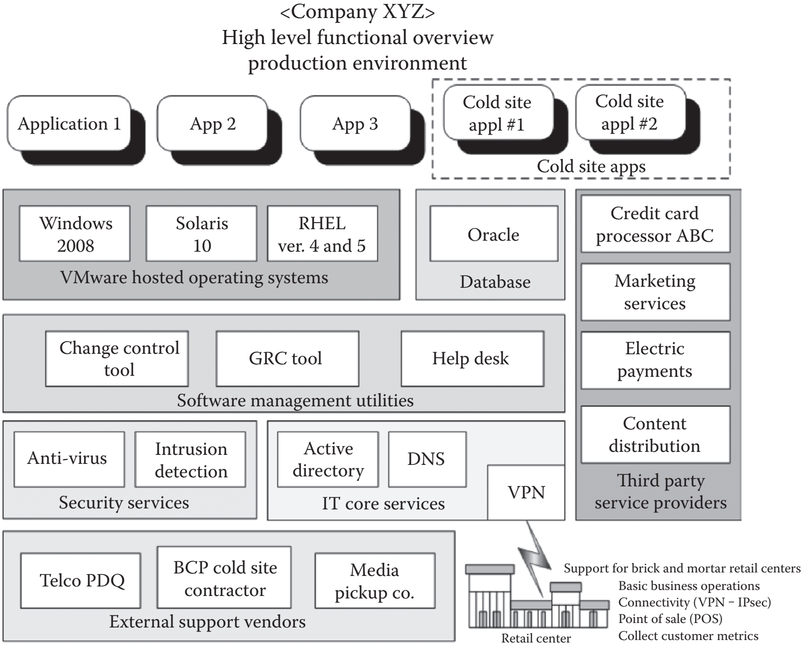


Figure 8.1 Operational environment functional overview.

Organizational Chart

As mentioned in the Purpose and Scoping section, your executive sponsor should provide an initial list of contacts for you to interact with that manage or support the business processes considered “in scope” for the project. Use this initial list of contacts to create a functional organizational chart. This simple tool will be referred to often and expanded often throughout the plan’s life cycle. Consistently, one of the first questions asked by many new members of the CoOP team is, “Who else have you talked to?” Having an organizational chart of the internal and external parties, which includes functional responsibilities, will streamline many conversations related to who is responsible for certain aspects of the environment. It will also serve as the basis for your communication plan. Figure 8.2 is a sample of a functional organizational chart for an IT-centric CoOP.

Compliance Obligations

This is a topic that should be near and dear to every security and compliance practitioner. As we often assert but don’t always achieve, here is our chance to make sure IT security and regulatory compliance’s needs are incorporated into the plan from the very beginning. Carefully review the data, assets, and business processes

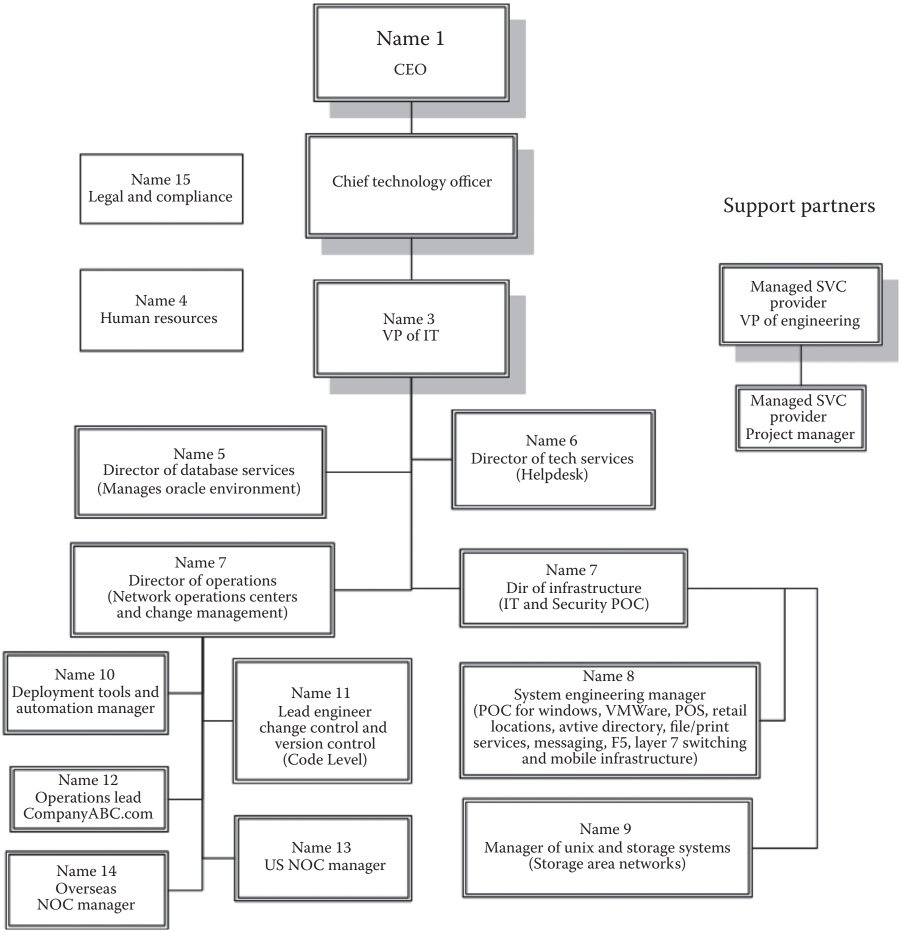

Name 1
CEO
Chief technology officer
Name 15
Legal and compliance
Name 4
Human resources
Name 3
VP of IT
Support partners
Managed SVC provider VP of engineering
Managed SVC provider Project manager
Name 5
Director of database services
(Manages oracle environment)
Name 6
Director of tech services
(Helpdesk)
Name 7
Director of operations
(Network operations centers and change management)
Name 7
Dir of infrastructure
(IT and Security POC)
Name 10
Deployment tools and automation manager
Name 11
Lead engineer
change control and version control
(Code Level)
Name 8
System engineering manager
(POC for windows, VMWare, POS, retail locations, avtive directory, file/print services, messaging, F5, layer 7 switching and mobile infrastructure)
Name 12
Operations lead
CompanyABC.com
Name 13
US NOC manager
Name 9
Manager of unix and storage systems
(Storage area networks)
Name 14
Overseas
NOC manager

Figure 8.2 BCP sample organizational chart.

to clearly understand the regulatory, compliance, and contractual mandates that must be maintained under normal operations and during DR operations. In addition to the previously described high-level narrative, add a dedicated section to the CoOP that establishes these important commitments and describes how you intend to meet them. A representative from legal or the compliance team, if your organization has one, will be very valuable in creating content for this carefully worded section. Articulating these requirements and the steps the organization intends to take to meet these obligations will be valuable when discussing the CoOP with partners, service providers, and other third parties. Expect it to be reviewed in great detail by individuals that oversee and verify compliance, including auditors and examiners from respective government agencies.

Example of the Compliance Section Building on the Previous Examples

The content, data collection, and associated activities for <Company XYZ>.com's web site have a material effect on the financial performance of <Company XYZ>. Implementation of any alternate site data processing or storage must maintain the same level of safeguards and data protection as the main data center.

All existing <Company XYZ> internal policies and procedures, including information security, ethics policy, and other human resources and workforce directives remain in effect during a declared event. This requires that all employees and supporting vendors maintain adherence to all agreements associated with nondisclosure and confidentiality.

These policies, procedures, safeguards, and compensating controls are required in part to maintain industry best practices and general requirements for compliance with the following:

- Gramm–Leach–Bliley Act (GLBA)
- Sarbanes–Oxley Act (SOX)
- European Union Data Protection Directive (EUDPD)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- {Add your favorite regulatory compliance initiative here}

<Company XYZ> expects to maintain the data security and confidentiality standards via contractual obligations with alternate location, services, and data storage providers (e.g., Company A, Company B, and Company C). These contractual obligations establish guidelines for performance by support providers, but do not specify tools, procedures, or technologies to achieve compliance demonstration. <Company XYZ's> vendor selection process and contracts management organization, supported by the IT department, have conducted due diligence on the service providers to evaluate, through staff interaction, presentations, site inspections, and executed contracts, a demonstration of adherence to best practices and use of industry certifications to support ongoing compliance requirements.

Summary of Critical Services and Essential Functions

To avoid any confusion or misunderstanding related to the resources and business processes that are being included in the CoOP, produce a comprehensive list of elements that will be provided in the event a disaster is declared. This serves two important purposes: (1) it explicitly articulates in technical or business terms what is in scope for the plan, and (2) it explains that during an emergency situation, many organizational capabilities may be suspended or rendered unavailable if they are not required to support critical business functions. Careful review of this section by all members of the CoOP team is crucial to verify that the services and capabilities they require are being incorporated in the recovery plan. For example, if a help desk is to remain viable during a disaster to support recovery operations, have items such as e-mail servers, telephones, service desk application servers, and workstations been provisioned? In many cases, this section will be revisited during postincident reviews as assumptions and capabilities are refined during plan testing exercises.

Example of the Critical Services and Essential Functions Section

Essential functions are those computing and connectivity capabilities that are minimally required to maintain and host <Company ABC's> critical applications.

- Critical services
  - Network connectivity
    - MPLS WAN network connectivity
    - VPN for retail locations and IT staff
  - Security policy enforcement
    - Firewall
    - Intrusion detection service (IDS)
    - URL filtering
    - Antivirus
  - IT core services
    - Active directory
    - DNS
    - DHCP
  - Virtual environment, OS, application, and database software
    - VMware ESX
    - OS platforms: Windows, Solaris, and Red Hat Linux
    - Oracle database
  - Operations Center (NOC) and help desk support
    - <Primary Production Facility>
    - <Secondary Production Facility>
  - Configuration management
    - Change management
    - Source code version control

If you are a fan of ITIL, you may have something to this effect:

Operationally, network and service management align with industry standards such as ITIL. These models separate IT management processes and functions into groups that drive a service management approach aligning the deployment and maintenance of IT infrastructure into meaningful services supporting business functions. As critical functions, only incident management, problem management, and a subset of configuration management and security management (focused on Internet access) is required to keep the network and critical applications running under emergency conditions.

Subsequently, all other functions and processes are not deemed necessary during an emergency or declared event. *These noncritical functions will stop under emergency conditions in order to allow resources to focus on the primary goal, during an emergency, of maintaining the critical applications and/or restoring connectivity to the main processing facility in* <Primary Production Facility or City>.

Contingency Operations

Now that we have established the scope, identified some threats, and gathered some of the technical details associated with the business processes we are tasked with protecting, it's time to develop operational plans to detect and react to a wide range of threats. These plans include the development of a series of steps to eliminate or minimize the damage caused by a disruptive event. There is a considerable amount of content in this section that establishes the foundation for implementing an effective CoOP program. Many organizations utilize the following sections as the basis for conducting an orientation session for new CoOP team members. This section is designed to establish common terminologies, define various Critical Incident Response Team (CIRT) roles and procedures that will form the basis of the organization's operational procedures to implement the CoOP program. For organizations that have an existing BCP plan that needs to be updated, try to map current terms and procedures into a similar operation framework that builds on historical terms and procedures. The goal should be to create a flexible and comprehensive process that mimics the capabilities described in this section. Organizations that do not have a plan to build on will have a bit more leg work to do as they establish new roles, procedures, and workflows to implement these program components.

Incident Response Process Overview

Note that a number of concepts in this section were adapted from the CERT Incident Management and Control document published on May 2010 (http://www.cert.org/resilience). It is a well-written document, sponsored and paid for by the U.S. Department of Defense, but tends to empirically lend itself best to large government agencies. The definitions and criteria are very good so they have been largely unchanged to allow for direct references back to the much more detailed text in the original publication. Additional content and consolidation of some topics have been undertaken to provide supplemental material that is more frequently encountered in commercial settings.

Detected Events and Declared Incidents

Incident management begins with event identification, triage, and analysis. An *event* can be one or more minor occurrences that affect organizational assets and have the potential to disrupt operations. An event may not require a formal response from the organization—it may be an isolated issue or problem that is immediately or imminently fixable and does not pose an organizational harm. For example, a user may report that they have opened an e-mail attachment and now their workstation is not operating properly. This "event" may be an isolated problem (e.g., event caused by malware) or an operator error that requires attention but may not require an organizational response.

Other events (or series of events) require the organization to take immediate action. Upon triage and analysis, these events may be the basis for a "declared incident" by the organization. An *incident* is an event (or series of events) that significantly affects the organization's revenue-generating assets or associated services. An event that results in an incident declaration requires the organization to respond in some way to prevent or limit any detrimental effect to critical assets or services.

For example, several customers may independently report that they are unable to place orders via the Internet (events). The problem is deemed to be caused by a DoS attack that is being targeted against the web portal (incident) that is preventing normal revenue-generating activities to operate normally. In this case, the organization must be able to recognize the attack, analyze the threat, and quickly develop a response to mitigate the effect of the incident.

The organization must be able to effectively monitor and identify events as they occur. In near time, they must be able to quickly determine when an event or a series of events constitutes an incident that requires a coordinated and planned response. To apply incident management processes, the organization must have a foundational structure for event detection, reporting, logging, and tracking, and for collecting and storing event evidence to support administrative or law enforcement activities.

The extent to which an organization can accurately identify the sources and intent of events improves its ability to manage incidents and their potential detrimental effects. At a minimum, the organization should identify the most effective methods for event detection and provide a process for reporting these events so that they can be consistently triaged, analyzed, and addressed. Staff should be assigned the task of monitoring various organizational processes (both technical and nontechnical) to identify and report events. Typically, the organization's service desk is often the front line for collecting event data and for commencing the incident management process.

The most likely sources and of methods of event detection related to the IT and security infrastructures include

- Monitoring of technical infrastructure (e.g., edge devices, network traffic)
- Reporting of problems or issues to the organization's service centers

These commonly come to the operations center via one of the following:

- Reports from the customer service team of end user problems
- Escalations from help desk reporting widespread or severe problems
- Notification from engineering that they have self-identified or been informed of a functionality defect in an Internet-facing application
- Observation of operations and line of business managers (e.g., normal routines and workflows don't seem to be operating correctly)
- Environmental and geographical events reported via media outlets
- Reporting from legal staff, law enforcement, or first responders
- Observation of a breakdown in critical business processes or asset productivity (e.g., higher than usual number of credit cards being declined)
- External notification from other entities such as ISP, security service providers
- Results of audits or assessments (e.g., PCI or vulnerability scan result)

Figure 8.3 illustrates some common events sources (external and internal).

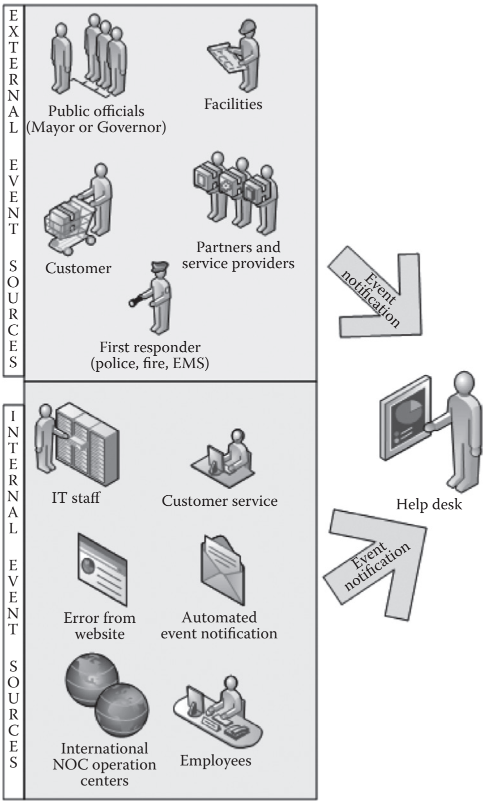

EXTERNAL EVENT SOURCES
Public officials (Mayor or Governor)
Facilities
Customer
Partners and service providers
First responder (police, fire, EMS)
Event notification
INTERNAL EVENT SOURCES
IT staff
Customer service
Help desk
Error from website
Automated event notification
Event notification
International NOC operation centers
Employees

Figure 8.3 Common event sources.

Event Detection and Documentation

Many organizations, even large, well-funded companies, may not have an effective method for capturing and cataloging disruptive events. The CoOP activity process probably isn't grounds enough to build a robust system from scratch; therefore, first attempt to adapt any existing help desk or event management workflows to support your program. In many cases, a less formal process for logging events as they are identified and tracked typically is handled by a traditional IT help desk. Identify and document how event logging and tracking is currently handled to see whether it is sufficient for your plan or if it can be adapted to ensure that potentially disruptive events are properly handled through the incident life cycle. Almost any logging and tracking capability can be leveraged to facilitate event triage and analysis activities, provide status updates on an active event, and may be useful in the postincident review processes when trying to identify trends and or performing a root-cause analysis on historical events. Logging and tracking may also be used to support forensic activities when done properly.

Logging and tracking procedures should allow for the possibility that some events will escalate into declared incidents. As a result, additional information will be collected as the incident proceeds through the incident handling life cycle and subsequent response activities.

According to the CERT guideline, basic information about events (and incidents) should include

- A unique organization-derived identifier (help desk incident number)
- A brief description of the event (type of event)
- Event category (physical or technical, based on categories predefined by the organization such as "denial of service," "virus intrusion," or "physical access violation")
- Organizational assets, business services, and organizational units that were affected by the event (including the seriousness of the organizational consequences)
- A brief description of how the event was detected, who identified the original event, and any relevant details about the operating environment currently being affected by the event (e.g., business process, partner/supplier connectivity, application, network segment, and operating systems)
- If the event has been escalated and is now a declared incident—indicate the individuals or teams to whom the incident was assigned for containment, analysis, and response
- Costs associated with the event or incident
- Relevant dates, times, and milestones (such as when the event or incident was first detected or when it first occurred)
- Actions taken thus far in response to the event or incident

Critical Success Factor—There are two points of view that should be considered related to event management and data collection. A derivative of the CERT parameters listed above is by far the most common approach because it easy to implement using a simple form(s) and minimal infrastructure to capture basic information that will suit most organizations (e.g., a web-based help desk ticket with a default assistance request form that is easily populated with basic information and predefined pull-down menus for the most common situations). Alternatively, some large organizations with very sophisticated response capabilities often take a different approach to event data collection and crisis management as illustrated in the book, *Business Continuity Management*, by Michael Blyth (eISBN: 978-0-470-47772-4), which provides a library of "Crisis Information Capture Reports" that are very precisely written to capture specific information based on the *type* of incident encountered. It is a very comprehensive approach, but would take considerable effort on an organization's part to integrate and train help desk staff on the wide range of incidents included in the library of scenarios. That being said, it is a very well thought out approach that reinforces that the *type* of information collected about an event can be largely dictated by the type of crisis being addressed. A suspicious package leaking a white powder being sent to a discrete data center mailroom and a distributed denial-of-service (DDoS) attack could both have detrimental effects on an organization's IT and business operations, but consider the type of information that would be useful to describe each threat for the staff that is responding to an activation of the CoOP. How well would a one-size-fits-all web form address the types of scenarios you anticipate could disrupt your operations?

Events Analysis and Triage

The triage of event is an analysis activity that helps the organization to gather additional information for event resolution and to assist in incident declaration, handling, and response. Triage consists of categorizing, correlating, prioritizing, and analyzing events. Through triage, the organization determines the type and extent of an event (e.g., physical versus cyber), whether the event correlates to other events (to determine if they are symptomatic of a larger issue, problem, or incident), and in what order events should be addressed or assigned for incident declaration, handling, and response. Triage also helps the organization to determine if the event needs to be escalated to other organizational or external staff (outside of the incident management staff) for additional analysis and resolution (e.g., Zero Day Attack).

Some events will never proceed to incident declaration if the organization determines these events to be inconsequential. For events that the organization deems as low priority or of low impact or consequence, the triage process results in the closure of the event, logging in the knowledge base, and no further actions are performed.

Events that exit the triage process warranting additional attention may be referred to additional analysis processes for resolution or declared as an incident and subsequently referred to the Incident Response Manager (IRM) for resolution. These events may be declared as incidents during triage, through further event analysis, through the application of incident declaration criteria, or during the development of response strategies, depending on the organization's escalation criteria, the nature and timing of the event(s), and the consequences of the event that the organization is currently experiencing or believe are imminent.

Declaring Incidents

Incident declaration defines the point at which the organization has established that an incident has occurred, is occurring, or is imminent, and will need to be handled by a cross-functional team (aka CIRT). Transition from event detection to incident declaration can be immediate, particularly when it is clear to the organization that there are significant detrimental effects on an organization's assets or associated services and a response is required to limit these events and their effects.

The actual time from event detection to incident declaration may be immediate, requiring little additional review and analysis. In other cases, incident declaration requires more extensive analysis. Each organization may need to establish predefined criteria developed from historical experience for threats that have a high probability of occurrence and significant detrimental effect to assist operational staff in determining when to initiate an immediate incident declaration. Specific guidelines are covered in detail in the Event Category and Response section of this chapter.

Once an incident has been declared, the organization will immediately perform additional analyses to develop and implement an appropriate action plan for responding to and handling the incident. This action plan may represent a routine activity (e.g., asking users to stop opening virus-infected e-mail messages, updating an IDS signature file, or implementing a new firewall rule) or a specifically designed response that is unique to the incident and requires significant levels of organization coordination and logistical support (e.g., notifying existing customers of the detection of a targeted phishing e-mail via the company web site, issuing a public press release, or contacting law enforcement).

Incident Declaration Criteria

There can be many unique factors that must be considered in determining when to declare an incident. Through experience, an organization may have a baseline set of events that define standard incidents, such as a virus outbreak, unauthorized access to a user account, or a DoS attack. However, in reality, incident declaration occurs on an event-by-event basis based on the context and potential to disrupt normal operations. To guide the organization in determining when to declare an incident (particularly if incident declaration is not immediately apparent), the organization must define incident declaration criteria (specific guidelines are covered in detail in the Event Category and Response section of this chapter).

These are examples of criteria that guide an organization's determination of whether to declare an incident:

- Is the event common in the organization? Has it occurred before? Did past occurrences of the event result in an incident declaration?
- Is the event isolated (i.e., only one user has reported it) or are there multiple occurrences of the same event being reported across the enterprise (through the service desk or similar construct)?
- Is the effect of the event imminent or immediate? Is the organization already suffering some effects from the event? Is there a crisis that has been precipitated by the event?
- Does the event affect the availability of core business drivers such as a high-value service that produces revenue?
- Does the event constitute a violation of organizational policy, fraud, or theft?
- Is the life or safety of employees or external entities at risk?
- Is the integrity and operability of a facility at risk?
- Is the integrity and operability of a high-value service or system at risk?
- Are there other organizational effects that are imminent or are already being incurred, such as damage to the organization's reputation?
- Is there a potential legal infraction or possible future legal (civil or criminal) concerns?

Analysis of an Event Resulting in a Declared Incident

Event analysis is primarily focused on helping the organization determine an accurate impact assessment so an appropriate impact category can be assigned. In most cases, events that are assigned an impact level of medium or high will result in the immediate declaration of an incident. Response to a declared incident is refined by the CIRT team by examining its root cause and the effects that have already been detected or are anticipated by the organization. Analysis is performed to further understand the intent of the originating entity or threat, to develop and implement action(s) to contain its effect, and to recover from any resulting damage. It should also help the organization to determine whether the incident has legal or regulatory compliance ramifications.

Incident analysis requires a broad range of skills from across the organization. Depending on the nature of the incident, analysis may involve asset owners, IT staff, physical security staff, auditors, legal staff, as well as external stakeholders such as vendors and suppliers, law enforcement, and vulnerability clearinghouses. Incident analysis may involve staff to whom the incident has been escalated or assigned to by the IRM.

Activities that may be performed to analyze the underlying events associated with a declared incident include

Internal sources of information

- Interviews with those who reported the underlying event(s), as well as those who are involved in its investigation
- Interviews of specific knowledge experts who have a detailed understanding of the area affected
- Interviews of asset owners for assets (such as information) that have been affected by the incident
- Review of relevant logs and audit trails of network and physical activity

External sources of information (request assistance as needed)

- Consultation of vulnerability and incident databases such as the US-CERT Vulnerability Notes Database and The MITRE Corporation's Common Vulnerabilities and Exposures List
- Consultation with law enforcement or first responders
- Consultation with contracted legal and audit staff
- Consultation with facilities or property management personnel
- Consultation with product vendors and software/hardware suppliers (if their products are involved)
- Consultation with emergency management staff (if the incident is a safety concern)

Organizational Response to a Declared Incident

The nature of a declared incident implies that the organization has already incurred some negative effect, however limited, that requires the organization to react. Responding to and recovering from an incident often requires four primary actions from the organization:

- Immediate limitation or containment of the scope and effect of the incident
- Implementation of an appropriate response to stop the ongoing or future effect(s) of the incident
- Repairing any remaining damage
- Restore organizational assets and services to the state in which they existed before the disruption

Responding and recovering may also require a carefully coordinated collaboration between organizational units and external entities (such as service providers). Significant planning efforts are required to co-manage handling incident logistics, particularly if the incident is significant, catastrophic, or would result in an extended outage of revenue-generating operations for the organization.

Incidents that the organization has declared and which require an organizational response must be escalated to those stakeholders who can implement, manage, and bring to closure an appropriate and timely solution. These stakeholders are typically internal to the organization (such as a standing CIRT or an incident-specific team), but in some cases, can be supplemented by external resources in the form of contractors or other suppliers.

Responding to incidents describes the actions the organization takes to prevent or contain the effect of an incident to the organization while it is occurring or shortly after it has occurred. The range, scope, and breadth of the organizational response will vary widely depending on the nature of the incident. Incident response may be as simple as notifying users to avoid opening a specific type of e-mail message or as complicated as having to implement the CoOP alternate processing location procedures that require the relocation of staff and critical services to a facility that is on another continent. The broad range of potential incidents requires the organization response capabilities include both simple quick-fix options and longer-lasting sustainable solutions.

Actions related to incident response include

- Containing damage (i.e., taking hardware or systems offline or by locking down a facility)
- Collecting evidence (including logs and audit trails)
- Interviewing relevant staff (those who are involved in reporting or analyzing the incident and those who are affected by it)
- Communicating status and remediation plans to stakeholders, including asset owners and incident owners
- Developing and implementing corrective actions and compensating controls
- Implementing continuity and restoration plans

Communicating Incidents

Miscommunications or inaccurate information about declared incidents can have dire effects that far exceed the potential damage caused by an incident itself. As a result, the organization must proactively manage communications when incidents are detected throughout their life cycle. This requires the organization to develop and implement a communications plan that can be readily implemented to manage communications to internal and external stakeholders on a regular basis. This plan should provide relevant information to these entities and control or limit the degree to which misinformation and conjecture can develop. It must also consider the needs of a wide range of stakeholders that have a vested interest in obtaining information about organizational incidents in a controlled and regular manner.

Stakeholders that may need to be included in an incident communication plan:

Always contacted during an incident

- Members of the incident handling and management team
- IT staff (if the target of the incident is the organization's technical architecture and infrastructure)

Could be contacted based on requirements associated with a specific incident

- Asset or service owners (if their asset is the target of the incident) and
- Middle managers and executives

- Business continuity staff (if they will be required to enact continuity or restoration plans as a result of the incident)
- Human resources departments, particularly if personnel safety is an issue
- Communications and public relations staff
- Support functions such as legal and audit
- Law enforcement staff (including federal agencies), if the incident may have criminal ramifications
- External media outlets, including newspaper, television, radio, and Internet
- Affected customers or upstream suppliers
- Local, state, and federal emergency management staff
- Local utilities (power, gas, telecommunications, water, etc.), if affected
- Regulatory and governing agencies
- Shareholders (via corporate communication with senior executive approval)

Declared Incident Closures

Incident closure refers to the retirement of an incident that has been responded to; there are no further actions required and the organization is satisfied with the remediation result. It also provides notification to those affected by the incident that it has been addressed and that they should not be subject to continuing effects. Incident closure is the responsibility of the incident owner or IRM. Only authorized staff should be permitted to close an incident. It should be immediately followed by a formal postincident review.

Postincident Review and Reporting

Postincident review is a formal part of the incident closure process. The organization conducts a formal examination of the causes of the incident and the ways in which the organization responded to it, as well as the administrative, technical, and physical control weaknesses that may have allowed the original event to occur. To be effective, postincident review requires the input of all relevant stakeholders in the incident management process. This includes those who

- Reported the incident
- Detected the incident
- Triaged and analyzed the incident
- Responded to the incident
- Were affected by the incident
- Had the incident communicated to them

Postincident review will include a root-cause analysis. As deemed necessary by the CIRT, tools and techniques may include cause-and-effect diagrams, interrelationship diagrams, causal factor tree analysis, etc., in support of creating a postincident analysis report. This report should detail the organization's recommendations for improvements in administrative, technical, and physical controls, as well as the incident management process. Any specific operational changes should be documented for easy reference by affected personnel (e.g., update to knowledge bases or help desk procedures to react to similar incidents in the future).

Areas that need to be addressed or could be modified after an incident:

- Update protection strategies and controls to protect assets and services from future incidents of similar type and nature
- Update policies to reflect lessons learned
- Update training for employees regarding the incident
- Revise continuity plans and strategies to protect and sustain services and assets
- Review and revise life cycle processes
- Review and revise asset-level resilience requirements, if necessary
- Revise incident criteria
- Develop standardized responses to common incidents
- Improve incident management processes

Plan Management and Updates

The BCP/CoOP should be reviewed at a minimum of once a year. If an incident has dramatically changed any operational procedure or protection mechanism, then the plan should be updated as part of the postincident response process.

At a minimum, the following management and control work products should be reviewed for ongoing applicability and accuracy:

- Event reports, including sources of event detection
- Incident management plans
- Incident response strategy
- Event and incident status reports
- Incident communications plan
- List of incident stakeholders (verify contact info)
- Incident management policies, procedures, standards, and guidelines
- Incident knowledgebase (e.g., help desk knowledge database)
- Event and incident evidence documentation procedures
- Incident declaration criteria
- Incident escalation procedures and categorization criteria
- Postincident analysis reports
- List of incident management process improvements
- Contracts with external entities

Critical Success Factor—It is very important to set the right tone for the post incident review meeting. The facilitator should open the meeting by stating that the objective is to improve the organization's ability to handle future incidents. The facilitator should highlight elements of the response that went well and suggest areas of improvement. Encourage participation and candid feedback, but carefully moderate any attempts to begin finger-pointing or transferring accountability because something didn't work well during a recent incident. Focus the discussion around the process, facilities, and technology elements of the plan to avoid any unnecessary stress associated with attacks directed at individuals, departments, or partner's capabilities/performance. Senior level HR or executives that can manage the meeting properly can help keep the exchange constructive.

For the remainder of this chapter, we will focus on the practical applications of what we have learned from publicly available and private sources regarding this point and begin to translate the theory into a practical program. Remember this advice from Sun Tzu relating to planning and preparation as you begin to develop your own CoOP:

> Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.

Practical Application of the CERT and NIST Guidelines

Any event, or series of events, can become the basis for a declared incident. The following sections are designed to provide common guidelines for classifying and developing a response for events likely to occur within the <Company ABC's> operating environment. As part of the incident response process, the IRM will need to make an assessment of the event/incident's effect and assign an appropriate severity level. This severity level will be based on the potential effect on the operations or reputation of the <Company ABC's> entities. An incident's severity level drives the immediate technical and long-term organizational response. The severity level is determined as part of the Triage and Analysis phase of the response plan. It is initially a subjective evaluation by the IRM as to the risk and potential effect an incident may have on the organization or ongoing <Company ABC's> revenue-generating operations.

As incident management activities and defensive actions are applied, subsequent event assessments may cause an event to be reassigned to a different severity level. For the purposes of this document, the focus will be *primarily* on medium to high-level events that would require an *incident declaration* with a CIRT response. The other severity levels (e.g., low) would typically be managed as part of normal operations by NOC or IT department personnel, but are described here for clarity and documentation purposes.

Figure 8.4 is a high-level overview of the event management process. Specific event categorization, response, and role-specific responsibilities for the CERT team are covered in details in subsequent sections of this chapter.

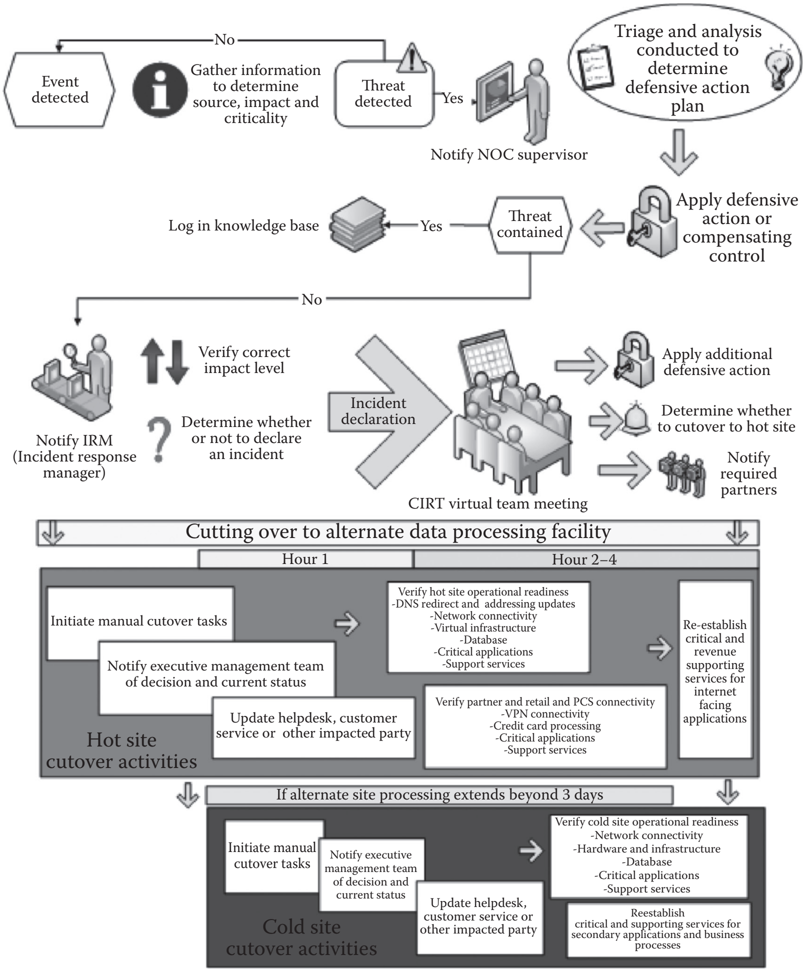

No
Event detected
Gather information to determine source, impact and criticality
Threat detected
Yes
Notify NOC supervisor
Triage and analysis conducted to determine defensive action plan
Apply defensive action or compensating control
Threat contained
Yes
Log in knowledge base
No
Notify IRM (Incident response manager)
Verify correct impact level
Determine whether or not to declare an incident
Incident declaration
CIRT virtual team meeting
Apply additional defensive action
Determine whether to cutover to hot site
Notify required partners
Cutting over to alternate data processing facility
Hour 1
Hour 2–4
Initiate manual cutover tasks
Notify executive management team of decision and current status
Update helpdesk, customer service or other impacted party
Verify hot site operational readiness -DNS redirect and addressing updates -Network connectivity -Virtual infrastructure -Database -Critical applications -Support services
Verify partner and retail and PCS connectivity -VPN connectivity -Credit card processing -Critical applications -Support services
Re-establish critical and revenue supporting services for internet facing applications
Hot site cutover activities
If alternate site processing extends beyond 3 days
Initiate manual cutover tasks
Notify executive management team of decision and current status
Update helpdesk, customer service or other impacted party
Verify cold site operational readiness -Network connectivity -Hardware and infrastructure -Database -Critical applications -Support services
Reestablish critical and supporting services for secondary applications and business processes
Cold site cutover activities

Figure 8.4 Event detection and incident response workflow.

Event Risk Categorization and Impact Guidelines

As part of normal business operations, events will be detected and reported by both internal and external sources. The technical teams and supporting management team need to conduct an initial assessment of the event to determine if it has the potential to disrupt the <Company ABC's> operating environment. As part of the event evaluation during the triage and analysis process, the technical team will evaluate an event to determine if it is a possible threat. The help desk or NOC personnel will assign an initial level of risk. Depending on the nature and source of the event, defensive actions or implementation of compensating controls will be deployed to offset the risk and potential effect. This could be as simple as updating an IDS signature file or implementing a new firewall rule. Evaluation of the residual risk associated with a specific event (post countermeasure implementation) will determine whether it should be escalated to the NOC manager. Upon consultation with the NOC manager, a decision will be made whether or not to contact the IRM.

As part of the incident response process, the IRM will need to verify the initial assessment of the event/incident's effect and assigned risk. *Declaration of an incident* will typically be reserved for events categorized as *medium* or *high* risk. Specific sources of physical and cyber/IT events as well as risks associated with regulatory compliance impact are included in the matrix below. In general, events that will be classified as medium or high risk will have one or more of the following characteristics:

- Any event that adversely threatens the confidentiality, integrity, or availability of the <Company ABC's> operating environment, information systems, or networks
- Any serious violation of the <Company ABC's> computer security or acceptable use policies
- Any violation of a mandatory requirement associated with a contractual, regulatory, or industry regulation
- Any unexpected or unauthorized change, disclosure, or interruption to the <Company ABC's> information resources that could be damaging to customers, partners, or the reputation of any covered <Company ABC's> entity

Risk and Impact Guidelines for Common Events			
Source of Risk	*High*	*Medium*	*Low*
Sarbanes–Oxley	1. Potential significant effect on revenue or earnings 2. Material effect on financial statements 3. Could result in serious fines or legal action—including request for litigation hold on business records 4. Potential significant business interruption 5. Could result in communication to Board of Directors if it occurs	1. Potential moderate effect on revenue or earnings 2. Potentially material to the financial statements 3. Could result in management letter from external audit firm (significant issue) 4. Failure to comply with legal or regulatory requirements in a specific instance 5. Potential business interruption 6. Should be communicated immediately to management	1. Slight to no effect on revenue or earnings 2. Not material to the financial statements 3. Not related to any major external audit findings or issues 4. Failure to comply with legal or regulatory requirements is not serious or an isolated case 5. Minimal business disruption 6. May need to be communicated to functional or business unit leader if it occurs

Risk and Impact Guidelines for Common Events			
Source of Risk	*High*	*Medium*	*Low*
PCI (leverage documents such as the PCI Self-Assessment Questionnaire to populate this section)	1. Electronic media discovered that contains unencrypted magnetic stripe (aka track) data for transactions no longer required for normal business reasons 2. External network vulnerability scan reveals internal IP address is reachable from the Internet 3. Unencrypted console access method discovered (e.g., telnet access) 4. Laptop that stored unmasked primary account numbers (PAN) on unencrypted portable media was stolen from an employee's rental car	1. Card holder data being transmitted with strong encryption key that hasn't been changed in 2 years 2. Encrypted VPN connection discovered between Development/QA and production environment 3. Laptop of recently terminated employee containing sensitive data was returned with the personal firewall disabled 4. Unencrypted copies of cryptographic keys used to create strong cryptographic keys found on a trusted employees personal laptop	1. Wireless access point discovered with default user ID and password enabled 2. Active user IDs discovered assigned to employees that are no longer with the organization 3. Insecure service (SNMP with default community string) discovered on system transmitting encrypted card holder data
HIPAA (leverage sources such as the HIPAA HiTech Act directives to populate this section)	1. Administrative credential on system containing Electronic Protected Health Information (EPHI) was compromised by a brute force attack initiated outside the institution's trusted network 2. Unauthorized active FTP connection discovered on Oracle database server used to store EPHI 3. Web site vulnerability assessment reveals that patient portal for major insurance provider is susceptible to SQL injection and cross-site scripting attacks	1. Wireless access using WEP encryption being utilized to transmit files that contain EPHI information 2. Two hundred and fifty patient paper records found in dumpster behind primary care provider office in a shared office park 3. VPN activity log reveals that a terminated employee user ID was accessed twice since they were separated from a primary care physician's office	1. System containing EPHI is not using current antivirus signatures 2. System containing EPHI is not to current OS and platform hardening standards 3. Shared user IDs being used by nursing staff in a primary care provider office for common area PCs 4. Weak passwords discovered during quarterly host vulnerability assessment

Risk and Impact Guidelines for Common Events			
Source of Risk	*High*	*Medium*	*Low*
Physical events (duration of outage dependent)	1. Severe storm that will affect the facility beyond carrier or facilities Service Level Agreements (SLAs) 2. Hurricane 3. Terrorist attack 4. Building bombing 5. Building fire	1. Tornado 2. Long-term utility or service provider outage 3. Chemical spill resulting in limited duration evacuation of facility 4. Water damage or facility flooding as the result of sprinkler failure or fire containment in adjacent areas	1. Short duration power outage or brownout that is expected to last less than 1 hour 2. Short duration water shortage 3. Short duration infectious diseases threat (stay at home recommendation for noncritical staff) 4. Property theft of device that may contain sensitive data on encrypted media
Cyber or IT events	1. Successful penetration and compromise of primary database by unauthorized user 2. Successful DoS attack with a significant effect on operations 3. Significant loss of confidential data 4. Loss of mission-critical application or system management tool 5. Admin or root user ID compromise 6. Illegal file server share or cross-site scripting detected 7. Site defacement that may have a significant financial or public relations effect	1. Penetration or DoS attack detected with limited effect on operations 2. Small number of systems compromised with no confidential data loss 3. Disruption of noncritical system or application for short duration of time due to network congestion or heavy traffic load 4. Widespread instance of new malware (e.g., virus/worm or botnet) that cannot be handled by IDS or antivirus solution 5. Detection of unapproved content with only a small risk of negative financial or reputation effect	1. Isolated instance of new virus or malware that cannot be easily quarantined or neutralized by IDS or antivirus solution 2. Significant level of network probes, scans, or similar activity of concentrated reconnaissance 3. Intelligence received concerning threats to systems that may be vulnerable (e.g., security patch or configuration change) 4. Penetration or DoS attempt with no effect on operations 5. Abuse of privilege *attempt* using a root or admin user ID 6. Individual system failure of a noncritical system or management capability

Risk and Impact Guidelines for Common Events

Source of Risk	*High*	*Medium*	*Low*
Interruption of payment processing	1. Payment processing suspended or interrupted for more than two hours 2. Fraud detection and notification by credit card issuer that may indicate targeted identify theft	1. Payment processing suspended for less than 2 hours 2. Credit and debit card declines on automated renewals increase beyond daily average	1. Credit card or PayPal transaction denials affecting less than 1% of daily expected revenue target 2. Temporary loss of connectivity to a single credit card issuer (transactions being held for final processing and reconciliation by member bank)
Source of cyber event seems to originate from client or business partner computing environment	1. Long duration, targeting activity is adversely affecting ability to conduct normal business transactions 2. Analysis indicates a compromise of critical asset is being attempted via automated scripting against specific infrastructure components 3. Countermeasures or compensating controls are not able to minimize effect or isolate sources to stop the inappropriate activity	1. Persistent activity having a limited effect on normal operations 2. Traffic or intensity of network activity increasing steadily and could result in degrading company asset performance	1. Limited effect seems to be an isolated incident 2. Limited duration that can be contained by existing security tools or compensating controls

Event Category and Response

As events are logged and evaluated by help desk and NOC personnel, an appropriate response is necessary to mitigate risk and minimize potential damage. This section describes the categories of potential effect, event characteristics, examples of representative events, and recommended organizational response(s). As mentioned previously, medium to high impact events require the attention of management and could result in a declared incident.

Event Category and Response Matrix			
Impact Level	*Description*	*Example Events*	*Action*
Low	These events are *not* expected to escalate or create a situation that would result in an incident declaration	1. Isolated reconnaissance by potential hackers 2. Password policy violation by an employee 3. Detection and removal of virus during a scheduled scan	1. Log utilizing existing system management and help desk procedures 2. No escalation or management notification required
Medium	Event has the potential to affect critical business activities or IT operations and may escalate into a declared incident	1. Repeated reconnaissance by potential hackers on from a single sources or IP Address 2. Malicious code or botnet attack blocked by existing security infrastructure or compensating control 3. Detection of deliberate and ongoing attempts to gain access to a system	1. Take defensive action as appropriate 2. Record critical incident information 3. Consult with NOC manager as part of triage, analysis, and countermeasure evaluation 4. Recommend whether to escalate or declare as an incident 5. Escalate to IRM
High	Event has escalated beyond a previous classification or has recently been discovered as having a detrimental effect on the <Company XYZ's> Internet-facing assets, the reputation of the organization, violates the organization's security policy, could potentially result in a violation of regulatory compliance, or result in adverse legal action	1. Unauthorized access or theft of data from sensitive systems (e.g., financials or client records) 2. Financial fraud detection utilizing any of <Company XYZ's> computers or resources 3. Improper use of high-level accounts such as root or administrator 4. Defacement of Internet-facing <Company XYZ's> web site 5. Successful DoS attack resulting against any network infrastructure, communications component, or revenue-generating resource controlled by <Company XYZ's> or a contracted service provider 6. Unauthorized modification of hardware, software, or configuration of a critical system 7. Theft of a computer system or storage device known or suspected of containing sensitive data	1. Capture event and incident data to provide to the IRM 2. Activate the incident response plan by declaring a high-priority incident 3. Initiate CIRT communication plan via call tree 4. Host CIRT virtual team meeting 5. Record events associated with incident sequentially 6. Identify any additional subject matter experts or support staff that could potentially be called upon to assist and, at the IRM's direction, ask them to participate in initial incident CIRT virtual team meeting

Event Category and Response Matrix			
Impact Level	*Description*	*Example Events*	*Action*
Business driven (medium to high)	Events could cause financial or reputational damage	1. Unusual or transaction that exceed predefined limits 2. Excessive disruption of normal financial services (e.g., high number of credit card declines) 3. Fraudulent activities detected by the business unit 4. Unusual system or customer activity reported by non-IT staff (e.g., customer service indicates a phishing scam e-mail has been sent to more than 25 customers)	1. Take defensive action as appropriate 2. Record critical incident information 3. Consult with NOC and business unit manager as part of triage, analysis, and countermeasure evaluation and decide whether to declare an incident 4. Escalate to IRM 5. If possible, refer to specific institutional guidelines as appropriate (PCI)

Response Team—Roles and Responsibilities

As potentially disrupted events are detected, members of the <Company XYZ's> IT department and the executive management team will be called upon to assist in evaluating the risk and in developing an appropriate response. This internal team is made up of technical employees, IT managers, <Company ABC's> executives, and supporting organizations such as hot, standby, and cold site service providers. This section describes the roles and responsibilities correlated with the three levels of impact. It is to be used in conjunction with any <Company ABC>-approved communication and distribution plans that designate specific employees and organizations corresponding with these roles. It is designed to be flexible; based on a wide range of potential threats and sources of assistance that the organization could call upon to deal with any declared incident.

Incident Response Team—Roles and Responsibilities		
Impact Level	*Staff Member or Team*	*Responsibilities*
Low	Help desk, NOC engineers, systems and network administrator	Real and near-time monitoring of all information assets and support services Initiate proactive or defensive action to protect against further effects of a harmful event

Incident Response Team—Roles and Responsibilities		
Impact Level	*Staff Member or Team*	*Responsibilities*
Low	NOC manager	Manage operational monitoring environment Receive and track incident data Determine effectiveness of initial defense action or compensating control Manage decision process initiate event triage and analysis required before event declaration Determine initial effect classification of an event(s) Contact the IRM if an event is detected that will result in an incident declaration of medium or high impact
Low to medium event escalation	NOC manager	Notify the IRM of details and determine if an event declaration is required Provide ongoing information to IRM on the effectiveness of defensive or ongoing countermeasure activities Review and update technical information provided by system administrators, help desk or customer service team Review incident response technical details and complete any outstanding fields Initiate logging and records collection to support CIRT virtual team recovery activities If employees or customers are affected by event, verify that on-duty help desk is aware of situation and operational effect
Low to medium event escalation	Help desk, NOC engineers, systems and network administrator	Provide continuous updates to NOC manager on the effectiveness of countermeasures or event containment activities Gather data and complete incident declaration form and forward to appropriate NOC and IT functional manager
Low to medium event escalation—triage and analysis activities	IRM (initially, a NOC manager until additional support or escalation is required)	Review incident declaration documentation and discuss current and short-term response with NOC manager Evaluate effectiveness of countermeasures and containment activities to determine if risk has been reduced to a low level Determine if event has been given proper impact classification As needed, initiate CIRT virtual team meeting (see Comm Plan) Assume responsibility for directing the incident response Notify senior executive team, if appropriate, of event declaration decision

Incident Response Team—Roles and Responsibilities		
Impact Level	*Staff Member or Team*	*Responsibilities*
Medium- or high-risk event has resulted in a declared incident	IRM (depending on the situation, the duties may be transferred to a more senior operations manager)	Verify content of incident response declaration form and distribute in advance of CIRT virtual team meeting Lead CIRT virtual team meeting to review event detection, ongoing response, and to gather input on best mitigation strategy Direct NOC manager or IT staff on remediation efforts Declare a primary <Company ABC's> partner facility that will be supporting production data processing and hosting in the short-term and long-term Notify vendors/external service providers as appropriate (e.g., hot site company, cold site company, off-site media storage company) Set short-term and long-term milestones to support any relocation activities Initiate any manual cutover activities required to restore services Provide help desk and/or customer service with periodic updates and set expectations for restoration of critical services Communicate activities to senior executive management Manage event through to reconstitution back to main data processing facility Collect artifacts and data that will be useful in postincident review activities

Alternate Facility Operations—Hot Site

The incident response workflow illustrates that, in some instances, an event will prompt the declaration of an incident that requires that business activities or IT operations will need to be transferred to an alternate facility to avoid prolonged disruptions. According to the Florida Business Disaster Survival Kit (www.fldisasterkit.com), here are the definitions associated with hot sites.

Hot Site—A site (data center or work area) provides a Business Continuity Management (BCM) facility with the relevant work area recovery, telecommunications, and IT interfaces and environmentally controlled space capable of providing relatively immediate backup data process support to maintain the organization's mission-critical activities.

Hot Standby—A term that is normally reserved for technology recovery. An alternate means or process that minimizes downtime so that no loss of process occurs. Usually involves the use of a standby system or site that is permanently connected to business users and is often used to record transactions in tandem with the primary system.

These types of facilities are experiencing very exciting changes in terms of capabilities and technology architectures that will make them viable for a much broader range of clients. Historically, hot sites were either maintained in another facility owned by the same company or contracted via a managed service provider to provide nearly identical hardware and operating environments to provide recovery services very quickly. For most companies and government agencies, the capital and operating cost to duplicate their most important business functions was beyond their financial means. Even as companies expanded globally, which should have facilitated the distribution of business operations across not just geographically isolated facilities but, in some cases, across continents, only a few were able to take advantage of this new opportunity to improve resiliency. Even if important issues such as localization (e.g., providing services and products in local languages) could be accomplished, the cost of duplicating hardware, slow connectivity links across long distances, and restrictive licensing by software and service providers, until recently, continued to hinder all but the largest organizations and government agencies.

The maturity of virtualization (e.g., hardware, software, and cloud computing) technologies, faster connectivity, secure remote access, and data aggregation capabilities is now affordable for almost every tier of organizations. The availability of these innovations is making the reality of having a standby capability available to almost every organization in any industry vertical.

Virtualization has many business benefits and even more potential returns as a mainstay in many organization's CoOPs. Many organizations have migrated many IT production facilities to heavily rely on this architecture. This has huge ramifications for organizations that want to maintain a hot standby or remote hot site capability. Hot standby environments are easier to achieve as the same management capabilities that maintain the production virtual computing environment are simply replicated and maintained in near-time at remote facilities. The same virtualization management tools that are used to maintain and update production virtual machines can be leveraged to quickly update in near-time, archived versions, or libraries of key server and client images. Using high-speed storage area networks (SANs), gigabit transfer speeds, and large amounts of RAM allocated to the process, security standards can be quickly maintained to the latest corporate standard for each virtual server or desktop instance including updates to operating systems, configurations, applications, and patches. Other organizations will simply choose to mirror a production facility with an exact virtual replica in an offsite location that can almost completely automate the synchronization of transaction-intensive databases or rapidly changing web content using dedicated tools that compensate for environmental conditions such as WAN latency, encryption at rest and in transit, and error correction in near real-time. Over time, this high-availability architecture will not only be the cornerstone of many CoOPs but will also provide additional benefits beyond fault tolerance and deliver increased application and service performance through true distributed processing, which supports higher transaction performance and quicker responses to distributed client requests. Additional availability benefits will be derived for other key hot site support activities as more media handling and secure storage is adopted in the cloud. Backup copies of key documents, forms, call list, vital files, application source code archives, and other electronic assets on secure, remotely maintained collaboration servers (e.g., SharePoint) will also speed up many of the recovery processes that historically relied on hard copy or portable magnetic media that only existed in a single physical location that could be difficult to reach during a natural disaster.

The global market demand for increased speed and resiliency of global telecommunication networks has also transformed the way organizations can design CoOPs. Dedicated, buried high-speed links between primary processing facilities and backup data centers will soon be eclipsed by dynamic, secure connections that can use sophisticated routing algorithms to bypass slow or unavailable paths in favor of less congested links over great distances. The ability to burst large amounts of data during off-peak periods, securely store data in the cloud, and dynamically build and tear down highly secure connection as needed across robust, fault-tolerant public networks can result in tremendous gains in performance, availability, and confidentiality for most organizations. These new capabilities across hardwired connections are complimented by advances in wireless technologies that add yet another layer of redundancy for the transmission and communication requirements of CoOPs. A CDMA or 4G carrier network connection may not be ideal network connectivity for normal transaction processing or e-mail traffic, but if it allows a critical business function to operate even at a reduced throughput, it may be sufficient to keep the business running for a short period.

The ability to communicate with CIRT team members has been affected even more dramatically by the proliferation of network and personnel connectivity options. Telecommuting has evolved beyond company-provided leased lines between specific locations and dedicated PBX systems that could only route calls to your primary work phone number. The proliferation of advanced portable technical capabilities carried by most consumers opens a wide range of communication and data exchange operations even if an organization's primary data and telecommunication facilities have been rendered inoperable. Most IT and management team members carry a smart phone device, can use personal devices to connect to corporate resources via approved VPNs, have access to private voice over IP if not video conferencing capability (Skype), personal e-mail accounts, multiple phone numbers, and free conference bridge services in addition to the capabilities provided by most companies. Even important communication tasks such as contacting CIRT team members via call trees or cascade systems have been automated via recent corporate investments in technologies such as unified communication and crisis management and alert services. This is especially true in university environments and utility companies in which communicating with entire student bodies or every employee has been highly automated in response to increased personnel safety associated with natural disasters or acts of violence.

There are some additional challenges that have emerged as a result of all these new capabilities that should be addressed by every organization as part of their CoOP process. As critical data or services are moved out of corporate-owned facilities or are being performed by business partners instead of employees, compensating controls need to be established to maintain the organization's security posture and demonstration of regulatory compliance. Carefully worded terms and conditions in vendor contracts and service agreements should explicitly establish ownership, custodianship, and accountability for critical topics such as maintaining computing environment standards and safeguards to meet appropriate compliance mandates. The legal, compliance, and purchasing professionals in your organization should be included in the due diligence and execution of these agreements. Consider including terms and conditions/clauses that protect your organization's right to inspect and verify that data and services are being provided according to agreed upon standards and guidelines. For example, if contracting with a service provider that is providing a multi-tenant virtual environment using shared hardware for use as a standby site, you should verify how critical tasks such as separation of data is maintained. It is best to explicitly address all key concerns in writing and maintain accurate records to avoid any confusion about roles or accountability responsibilities. Your CoOP should include provisions with all key vendors to address data loss (e.g., lost or stolen media), security and compensating controls, incidents handling, and computing environment maintenance activities while operating at an alternate processing facility. Carefully consider the complexity and logistics of maintaining your production environment capabilities within the confines of someone else's managed facility (e.g., management reporting, exception handling, VPN access for IT and development staff, virus protection, IDS, OS hardening, applying patches, reviewing activity logs, application performance management, and database maintenance activities) can quickly become overwhelming and very cumbersome if not properly planned for proactively.

Critical Success Factor—It is very important to consider two things very carefully before implementing a hot site environment. (1) If there are weaknesses in critical security processes or procedures, they will likely be *amplified* or get worse when migrated to a virtual implementation. Consider how difficult it will be to address topics such as threat management, role-based access control, change management, data loss prevention, backup, and recovery if these tasks are further abstracted beyond company-owned facilities that you cannot secure via additional compensating controls (e.g., physical access, employee badging). (2) If you plan to migrate data, services, or business processes into a third-party facility, shared virtual environment, or cloud-based architecture, make sure there is a method and procedures to migrate it back to within your organization's control if you need to switch vendors or if you are not happy with that facilities' performance.

Alternate Facility Operations—Cold Site

There exist some business cases that require some organizations to still maintain cold sites. Considering the benefits of modern standby virtual architectures for IT components, it is expected that they will be less frequently utilized moving forward. For organizations that have determined that the sensitivity of data, specific hardware or equipment (e.g., manufacturing or printing), or where physical security is paramount, a cold site may be your only option. There are third parties that can be contracted to provide these services if your organization doesn't have the facility or capacity. In most instances, every operating cost and capital expense is at least doubled to keep the two facilities in sync. For this reason, many industries will set up "reciprocal agreements" with similar business partners to pool resources or distribute the cost of equipment if the collective requirements can be satisfied with universal components. A great example is when utility companies (e.g., electrical) operating in different states set up agreements to assist with recovery efforts if one is struck by a natural disaster and a similar capability can supplement repair and restoration activities (e.g., linemen, bucket trucks, generators, and trailers).

The other consideration with cold sites is that in many cases the recovery process takes significantly longer than hot or standby sites. Setting up hardware, loading software (OS, application, data) from portable media, and patching to current corporate standards is labor-intensive and may be complicated if physical access to the cold site is hampered by bad weather, limited transportation options, or significant distance away from the primary production facility.

Reconstitution to Primary Facility

After an incident has been addressed, the primary processing facility has been deemed safe to resume operations, and appropriate steps have been taken to prepare it for resumed processing, then reconstitution activities to the primary facility can proceed. These procedures can be generally described in the CoOP but, in practice, typically involve very specific operational and technical procedures to maintain proper sequencing to reestablishing capabilities in a specific order of tasks that enables foundational elements, verifies operating capabilities of internal and partner connectivity and capabilities, and establishes synchronization between environments before cutting back over to the primary processing facility. For many organizations, this will be a series of manual and automatic tasks and procedures that are frequently performed in a reverse sequence of the hot or cold site cutting over.

Postincident Review and Response Evaluation

Upon the completion of reconstitution, and once normal operations have been reestablished, it is very important that the CIRT and any affected parties evaluate the performance of the organization and its partners in responding to a declared incident. The following sections contain a framework of the topics that should be discussed and evaluated. Additionally, there is an optional section related to performance metrics that may be requested by senior management as part of the postincident review to quantify performance, impact, or associated cost of improving the organization's response capability. The content in these sections was adapted from the CERT Resilience Management Model version 1.0 and various NIST publications.

Incident Review Report Template Topics

Preparation

1. Were the location and supporting procedures to invoke the BCP/CoOP easy to access and known by all required parties?
2. Could more education of users or administrators have prevented the incident altogether or minimized the effect?
3. Were all of the people who needed to respond to the incident familiar with the incident response plan?
4. Were any actions that required management approval clear to participants throughout the incident?
5. Did the available staff have sufficient skills to do an effective job of responding to the event?

Event Identification/Detection

1. Does the organization know exactly when the initiating event first occurred?
2. How soon after the incident started did the organization detect it?
3. Could different or better logging have enabled the organization to detect the root cause event sooner?
4. How was the initial event detected?
5. How was the event routed to the help desk or NOC?
6. Should the event have been detected sooner by other monitoring capabilities currently in place?
7. Were the technical/business processing activities being effectively monitored, including exception handling?

Communication

1. Were the appropriate people available when the CIRT virtual team meeting was initiated?
2. Did technical staff effectively document all their activities to facilitate the initial CIRT virtual team meeting?
3. Were appropriate individuals outside of the standing incident response team notified and available for the CIRT virtual meeting?
4. Were incident details communicated appropriately to stakeholders at a level commensurate with their involvement (e.g., executive management)?

5. Which communications channels were most effective or helpful?
6. Which communication channels were rendered inoperable or ineffective during the declared event?
7. Did all the information flow from the appropriate source?

Response

1. How smooth was the process of invoking the incident response plan?
2. How well did the organization follow the plan?
3. Was the initial impact level correctly assigned on initial event detection?
4. Were originating events properly identified and logged?
5. Were proper procedures used to collect supporting technical and countermeasure effectiveness results?
6. Were disruptive events efficiently triaged and analyzed for root causes?
7. Was the incident properly declared according to the plan and response criteria?
8. Was the incident response properly escalated to designated stakeholders?
9. Did the initiating event originate from a known source of vulnerability or was it a new attack vector/unanticipated disruption?

Containment

1. How well was risk mitigated/damage minimized once the originating event was accurately identified?
2. Were preventative controls applicable to the originating event working properly?
3. Did any other compensating controls assist with the containment?
4. Did the compensating controls meet their stated intent in support of resilience or failover requirements?
5. What environmental conditions allowed the originating event to occur?
6. Did the available staff have sufficient skills to do an effective job of containment?
7. If there were decisions made on whether to disrupt service to internal or external customers, were they made by the appropriate people?
8. Are there changes that could be made to the environment that would have made containment easier or faster?
9. Was there an easy and effective method for technical staff to document all of their activities in support of ongoing CIRT activities?

Recovery

1. Was the recovery complete?
2. Was any data permanently lost?
3. Was there sensitive data that will likely never be recovered?
   i. Are there any associated mandatory reporting requirements?
4. If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities, and did the decision process follow the incident response plan?

5. Was a postincident review performed to improve the process?
6. Were proper forensics procedures used to collect and preserve evidence in the event data needed to be handed over for administrative procedures?
7. Do any changes need to be made to administrative, technical, or physical controls to improve BCP/CoOP response capabilities?

Incident Management Performance Metrics

An organization may elect, as part of their BCP/CoOP, to collect specific performance metrics to evaluate the benefit and effectiveness of the organization's ability to meet management-defined operating objectives. Senior management should evaluate the data collection and reporting capabilities associated with the BCP/CoOP to provide effective oversight and performance validation.

The following represents a set of operating parameters and metrics that may prove valuable to monitoring and evaluating the ongoing performance of the organization against the CoOP.

- Percentage of operational time that high-value services and assets were unavailable (by both users and customers) due to declared incidents
- Percentage of incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds
- Number and percentage of events or incidents handled in a specific period
- Number and percentage of events or incidents that are contained in a specific period
- Percentage of incidents that require escalation
- Percentage of incidents that require the involvement of law enforcement
- Number of events or declared incidents that have been logged but not closed
- Average time between event detection and incident declaration, response, or closure
- Percentage increase in the volume of events and declared incidents in a specific period
- Extent of consequences to the organization due to incidents by incident type (also referred to as magnitude; often provides insight into the difficulty to detect and remediate damage associated with specific events)
- Percentage increase in the elapsed time of the incident life cycle by incident type (the goal is to determine if a particular event or incident is more difficult than another to handle)
- Number and percentage of recurrence of specified events or incidents (look for patterns)
- Percentage increase in resource needs (training, skill building, technology investments, or additional FTEs/contractors) to support the incident management program

- Number of post-incident review activities that resulted in control changes or improvements to the CoOP process
- Number of risks in which corrective action is still pending (by risk rank)
- Level of adherence to process policies, number of policy violations, number of policy exceptions requested, and number approved
- Number of process activities that are on track per remediation plan
- Resource needs to support the remediation process
- Costs to implement the recommended changes

CoOP Review Exercises and Testing Procedures

> However beautiful the strategy, you should occasionally look at the results.
>
> **—Winston Churchill**

Establishing the initial BCP/CoOP is an important early milestone for protecting an organization's business interests. To be effective, the plan and supporting activities need to be maintained via a vigilant performance review life cycle consisting of ongoing updates, adaptations, and practical exercises to verify the program's effectiveness. Employee orientation training, active participation in tabletop scenarios, and practical drills will provide an environment for CIRT team members to understand assigned roles and responsibilities while simultaneously building confidence in response capabilities in a controlled environment. Partner and supporting organizations should be invited to participate in at least one annual test of the procedures to verify that contact information, contractual arrangements, and response capabilities support and meet your organization's SLAs and recovery windows.

Employee and Partner Training and Test Procedures

There should be at least an annual tabletop and practical test of the BCP/CoOP. Below is a list of the minimum training for all critical members of the CIRT.

CIRT Team Member Orientation

This is an overview of the business continuity/continuity of operations program. Each CIRT team member should attend once per year. This should explain the plan from conceptual overview, event sources, incident declaration, prioritization, communication plan, response procedures, hot and cold site capabilities, and restoration plans. It should include role-specific responsibilities for each CIRT team member.

CIRT Team Tabletop Exercises

Shortly after the completion of the CIRT team member orientation, the entire team should participate in a tabletop exercise with a focus on handling a wide range of scenarios utilizing approved recovery strategies. Leaders (IRM) from both the primary production and secondary facility should lead some of the tabletop exercises to verify an understanding of the roles, response and escalation procedures, and long-term support responsibilities.

Testing Scenarios

The event category and response matrix is an excellent source of scenario materials as well as any historical organizational events that result in a declared incident. Additionally, NIST Publication *800-61 Computer Security Incident Handling Guide* rev 1 provides a wide range of scenarios and supporting technical information related to response and technical considerations that would prove valuable during this training. This is available at http://csrc.nist.gov/publications/PubsSPs.html.

Specifically, the following scenarios, located in Appendix B of the NIST document, would serve as relevant training material for many CIRT teams:

Scenario 1: Domain Name System (DNS) Server Denial of Service
Scenario 3: Worm and DDoS Agent Infestation
Scenario 4: Use of Stolen Credit Card Numbers (Business Generated Event)
Scenario 5: Compromised Database Server
(Could be expanded to highlight regulatory compliance consequences)
Scenario 8: Outbound DDoS Attack
Scenario 10: Hacking Tool Download
(Highlights enforcement of Appropriate Use Policy and HR Involvement)
Scenario 12: Telecommuting Compromise
(Could be customized to reflect VPN connectivity and supporting remote facilities)

Functional Exercise

Hands-on testing of hardware, connectivity, and partner support capabilities to alternate processing facilities should be carefully rehearsed before testing in the production environment. Scenarios should be adapted from the tabletop exercise and based on the most likely and disruptive events established in the *Risk and Impact Guidelines for Common Events* for your organization. It cannot be emphasized strongly enough how important proactive communication and coordination across employee and partner organizations is before and during functional exercises. Every effort should be made to minimize even the potential effect on normal production and revenue-generating activities. Permission from senior management should always be received in writing before any functional exercise. Methodical record-keeping, event and activity sequencing, rollback procedures, milestones, checkpoints, and alternate communication channels should be established for each functional exercise.

Plan Reviews

Annual plan reviews, tabletop, training, and functional exercises should be recorded as part of the ongoing management of the CoOP life cycle. This is an important activity that is a regulatory requirement for some organizations. For each plan review, the following information should be captured:

Plan Holders

Enter the dates when plan reviews were conducted.
Incident response team leader (name)
Alternate team leader (name)
(Name)
(Name)
(Name)
(Name)

Training/Exercises

Enter the dates and number of participants for each activity. Each exercise type is expected to be conducted at least once per year.

Activity Date	*Conducted*	*Comments*
Orientation		
Team exercise		
Team leader		
Functional exercise		

CIRT team leaders: attach participant sign-in sheets, evaluations, and comments to meeting notes to document ongoing inclusion of relevant parties and maintenance of the plan.

Common Appendixes and Supporting Documents

There are many additional data sources, artifacts, and documents that can be used to supplement an organization's CoOP. Call trees, contact lists, network architecture diagrams, equipment inventory and configuration, backup or hard copies of critical device configurations, manual cutover procedures, and related documents are the most common. If creating the plan for the first time, remember to leverage artifacts and content created in previous sections. For example, utilize the functional organizational chart as the basis for your contact list and call tree if necessary. As part of the annual review or testing exercises, take every opportunity to verify that the plan and its contents are up-to-date because personnel, roles and responsibilities, business practices, and new business partners change frequently in most organizations.

Chapter 9

Access Controls

Kimberly Logan

Contents

Access Control

To begin to discuss access control, we need to understand what it really means. We all encounter access control every day without even realizing it. We lock our doors when we leave our homes, use PINs to access ATMs, and use badges to access certain areas of our work environment. The reason we do these things is that we have something of value we want to protect. Understanding this value is central to determining the level of access control necessary to protect it. This necessity makes it imperative for a business to classify its data if proper access controls are to be put into place.

Maybe you own a home in a residential neighborhood. Of course, you want to protect your belongings, so you lock your doors when you leave your home. You may even have an alarm system installed to notify you if anyone tries to break in. In this neighborhood, you probably wouldn't go so far as to install bulletproof windows or have an armed security guard stationed outside your home. You lock the doors of your car when you park it in your driveway and you may even leave lights on when you are away in the evening. You may give a trusted neighbor a key to your home, but do you share the code to your alarm system? You may not trust anyone but family members with your alarm code.

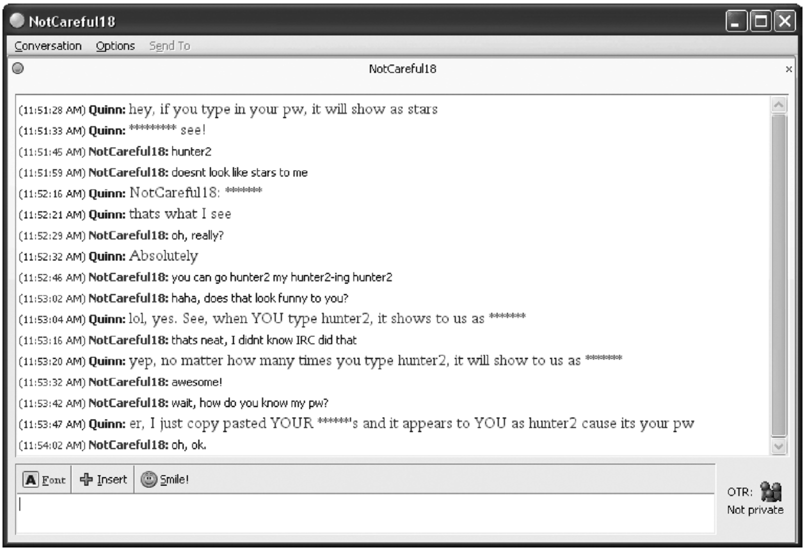
Access control is practiced all the time and is fundamental to information security. It is about the systems that protect valuable items and it is about the decisions made by people who determine who receives access. Access control can be used to control access to both physical spaces and areas and information within an information system. In a perfect world, people would have access to only those spaces or information that was required to do their job. However, in today's society, with workers having to wear more hats, it is easy for the lines to become blurred and it is much more difficult to get a good handle on effective access control.

In the article, "How safe is your data?" Brian Cleary points out the principle of least privilege, which plays a large part in access controls (Cleary 2008). This principle states that every person should have the least amount of access necessary to do their job. Least privilege applies to all areas of access control. Just because you give a trusted neighbor the key to your house so he can bring in your mail, doesn't mean that you will also give him your ATM PIN.

Another basic access control concept is the separation of duties. This concept means that more than one person is required to complete a task. ISO 27002 supports this principle in its requirement for an access control policy (ISO 27002:2005), and this is often an excellent principle to enforce when people are working with very sensitive information.

Access controls support the core security principles of confidentiality, integrity, and availability (CIA) by requiring users to positively identify themselves and verify that they possess appropriate credentials as well as the necessary rights and privileges to obtain access to the target system and its information.

When you've determined what you want to protect, the next step is to determine the appropriate type of access control to use to protect it.



```
(11:51:28 AM) Quinn: hey, if you type in your pw, it will show as stars
(11:51:33 AM) Quinn: ********* see!
(11:51:45 AM) NotCareful18: hunter2
(11:51:59 AM) NotCareful18: doesnt look like stars to me
(11:52:16 AM) Quinn: NotCareful18: *******
(11:52:21 AM) Quinn: thats what I see
(11:52:29 AM) NotCareful18: oh, really?
(11:52:32 AM) Quinn: Absolutely
(11:52:46 AM) NotCareful18: you can go hunter2 my hunter2-ing hunter2
(11:53:02 AM) NotCareful18: haha, does that look funny to you?
(11:53:04 AM) Quinn: lol, yes. See, when YOU type hunter2, it shows to us as *******
(11:53:16 AM) NotCareful18: thats neat, I didnt know IRC did that
(11:53:20 AM) Quinn: yep, no matter how many times you type hunter2, it will show to us as *******
(11:53:32 AM) NotCareful18: awesome!
(11:53:42 AM) NotCareful18: wait, how do you know my pw?
(11:53:47 AM) Quinn: er, I just copy pasted YOUR *******'s and it appears to YOU as hunter2 cause its your pw
(11:54:02 AM) NotCareful18: oh, ok.
```

Figure 9.1 Example of a hacker attack.

The three groups of access controls are preventive, detective, and corrective (PDC) and within each group are three types: physical, administrative, and technical. Each is just as important as the other. Used together, they provide defense-in-depth, which is what any effective information security program should strive to achieve. Defense-in-depth means that no one type of control alone is enough to stop the bad guys. Using a selection of controls that will be most effective for the given situation will provide the best security. Attackers will never stop trying and they can get very creative. Figure 9.1 (Hughes 2005) is an example of a creative method an attacker used for obtaining a password through an Internet Relay Chat session. It is a social engineering attack, but proper access controls could have helped the victim avoid this embarrassing situation.

Access Control Systems

Access control systems are put in place to ensure that only authorized individuals have access to information and that the information remains intact and available when needed. The purpose of access control systems is to prevent the modification of information by unauthorized users, allow the modification of information by authorized users, and to preserve the internal and external consistency of the data.

To accomplish this, controls are implemented. Controls help mitigate risk and reduce the potential for loss (Krutz and Vines 2003). Controls follow the PDC methodology and combinations of controls are required for defense-in-depth. An organization needs to consider the value of what it is trying to protect before deciding how much money it is willing to spend on controls. Preventive controls are used to inhibit harmful occurrences. Firewalls are an example of a preventive control. System logs are an example of detective controls, which are used to discover harmful occurrences. A documented procedure for cleaning a virus from an infected machine is an example of a corrective control, which is put into place to restore systems that have already been harmed by an event.

Although the previous paragraph categorizes controls by what they do, another way of categorizing access controls is by describing the way they are implemented, or what they are. The three different kinds of implementation are administrative, physical, and technical/logical.

Administrative Controls

Administrative controls include policies and procedures, awareness training, background checks, vacation history review, work habit checks and, in some cases, increased supervision. Administrative controls are very good for dealing with insider threats. Although nobody really wants to believe anyone they work with could be capable of such things, insider theft is rapidly growing. A 2007 study by Price Waterhouse Coopers (Aldhizer 2008) estimated that insiders were involved in 69% of database breaches. As the workforce becomes more mobile, as it is beginning to do and inevitably will become more so, it is imperative that businesses implement strong access controls to protect their most valuable information. Security awareness training can't be stressed enough and the need to be observant plays as critical a part in information security as do the chosen physical and technical controls. The user account termination policy is another administrative control that is extremely important in mitigating insider threats. This policy addresses accounts that are left active after a user is terminated from the company. In many cases, companies will notify Information Security to terminate accounts in the event of an unfriendly termination, but all too often they forget to do so when a once trusted employee simply resigns. The business doesn't recognize the threat or chooses to believe a threat doesn't exist.

Physical Controls

Security guards, security cameras, securing of server rooms, locking of laptops, and separation of duties play an important part in deterring what might have been a disastrous event had the controls not been in place. Think about it this way—would you be as tempted to sneak out of the office with a laptop in tow if you knew a security guard had his eye on everyone entering and exiting? Would you be as likely to try and download confidential information or enter a sensitive area of the building if you knew security cameras were watching? If you have to enter via a locked door to get to a server room, you'll probably avoid it in favor of something easier to access. It is human nature to choose the path of least resistance.

Technical/Logical Controls

These are probably the controls most people think about when they think about access controls. Controls such as encryption, smart cards, access control lists (ACL), software packages like ACF2 and RACF, biometrics, and transmission protocols. Technical controls restrict access to systems and protect the information the systems contain. I'll refer you to Chapter 3 for a discussion of encryption, but for access control purposes, laptops and USB drives should be encrypted. As part of my current work responsibilities, I put out a weekly awareness newsletter for the university community and without fail, every week, there are stories about lost and unencrypted USB drives containing sensitive information or someone who had a laptop full of personally identifiable information (PII) stolen from their car. Did I mention it was unencrypted? Attackers will keep trying, but we don't have to make it easy for them.

Through a risk-oriented approach to access control, we can achieve defense-in-depth that is appropriate for the information of value to the organization.

Access Control Models

The primary access control models are mandatory access control (MAC), discretionary access control (DAC), and role-based access control (R-BAC), which may also be referred to as nondiscretionary access control.

Mandatory Access Control

MAC is a very powerful and complex model in which permission is granted by system policy. Currently, it is most often found in highly secure government installations (Peltier et al. 2005). It relies on sensitivity labels for data as well as the classification levels for users. In most government installations, the classification levels are top secret, secret, unclassified, sensitive but unclassified (SBU), and confidential. When a user's clearance level is at or above the classification level of the data he or she is attempting to access, the system grants access. Most private sector businesses tend to use either DAC or R-BAC.

Discretionary Access Control

DAC is probably the most common access control model. Discretionary access permissions are identity-based. With DAC, all objects have an owner and access permissions are granted by the owner. Windows is an excellent example of DAC. When you create a file in Windows, you become the owner by default. You can read and modify the file, but unless you grant access permissions to someone else, they cannot access your file. Sometimes, the owner is a group rather than an individual, such as when an ACL is maintained and you must be a member of the group to access certain information. In this case, the entire group can access the information and has the same access permissions.

Role-Based Access Control

R-BAC, sometimes referred to as nondiscretionary access control, is a type of access control in which a user is assigned access based on their job description. This is a good model for companies where there are frequent personnel changes or for a bad economy where often consultants are used on a short-term basis in place of permanent employees. In high turnover environments, users are easily added to and removed from roles. As explained in "Practical Role-Based Access Control" (Galante 2009), R-BAC works well for companies with formal job structures. This occurs when employees' roles, documented job responsibilities, and job descriptions closely resemble reality. It should be organized, but not cumbersome. Organizations that have experience with Enterprise Resource Planning (ERP) security will find that most of it is a good example of role-based access control. Each user in the system is assigned a role or multiple roles required to do their job. Each role has access to transactions. When a user transfers departments, roles can be reassigned. If a user leaves the company, roles can be removed. One of the primary problems with this type of access control is aggregation. If a user transfers to a new group but retains any part of their job responsibilities from the previous position, they will either have too much access due to retaining unnecessary roles or new one-of roles will need to be created. This can create a maintenance nightmare.

No access control model is perfect for every situation, and organizations need to consider their business model and culture to determine which will work best for them.

User Access Management

User access management is about making sure authorized users have appropriate access to the system and preventing unauthorized system access. ISO 27002 outlines several areas where user access management must be considered. These areas include (1) user registration, (2) privilege management, (3) user password management, and (4) review of user access rights (ISO 27002:2005).

User Registration

User registration is also known as user account authorization, but whatever you call it, it is one of the most important pieces of the access process. User registration is the way users establish access to the system and also determines the access the user will have once on the system. User accounts provide accountability.

There needs to be a formal process in place for users to request access to the system. This process should include approval by an authorized party for the user to obtain access and the user should be required to sign a user agreement stating that they understand their responsibilities for the use of the account. A policy should also be in place and users should understand that all user IDs must be unique and each user may have one and only one user ID for each system. The documentation pertaining to the creation of a user account and access granted to the account should be retained as long as the user is an active employee in the same department.

Just as user registration and the surrounding processes are important, so are the processes implemented for user account removal, or deregistration. You may need to join forces with your HR Department or whoever else needs to be involved, but it is imperative that you have strong processes in place to ensure that when an employee leaves, the account is terminated. These processes should be documented, made known, and followed.

It is important that area managers inform Information Security or the administrators responsible for the removal of user accounts even when an employee leaves under more friendly terms. It is important to terminate the user accounts quickly and to ensure that access is removed from all the systems to which the employee had access. Unfortunately, when circumstances are less dramatic, people often don't think about the effect of leaving a user account available on a system. This is why it is important to do regular reviews to look for any accounts that have been unused for a specified period and inactivate those accounts. A typical time period used by many organizations is between 180 and 270 days.

Privilege Management

Very often in a business environment, users will have shifting job responsibilities and it is common for access levels to accrue to meet the new responsibilities without being adjusted to remove access that is no longer necessary. This phenomenon was referred to by Cleary as entitlement inertia (Cleary 2008). Unfortunately, failure to adjust privileges with changing job responsibilities can also lead to separation of duties violations or simply present excessive access issues. It is common for a business to want to grant high levels of access to a user who is very knowledgeable about a system, thinking that person can then be more helpful and more productive. Sometimes, the organization even has the employee continue to perform both the old and new job functions for a time. The business fails to consider that they have now put this user in a prime position to commit insider theft. The principle of least privilege should be applied to systems when granting user access—always grant the least privilege necessary for a person to perform their job functions. Whenever possible, an employee starting a new job should be relieved of their old job responsibilities and the access those responsibilities required. Having a trained backup for critical positions makes this process much simpler. Access reviews should be performed on a regular basis, with excessive access being removed. In any case, where elevated access is required, a documented and approved business reason should be kept on file and reviewed at regular intervals to ensure that it is still required.

User Password Management

Passwords have long been the keys that open the doors to the systems. Passwords have probably also been a point of contention about as long as they have been around. How long should they be? How often should they be changed? Why do I have to remember so many of them? I was going on vacation and my boss said I needed to give him my password, is that a problem? These are all questions that have been heard countless times throughout my information security career. Today, some people are even questioning the value of passwords as authentication mechanisms. These people need to keep in mind the information security tenet of defense-in-depth.

Businesses today should be enforcing strong passwords on their systems because we know that the stronger the password, the more difficult it is to crack. More difficult doesn't mean impossible, but combined with a regular password change period of no more than 90 days, it does make it much more difficult. There are many guidelines for selecting strong passwords. The most common state that they should be at least eight characters in length, not based on any dictionary word, and should contain a combination of uppercase and lowercase letters, numbers, and special characters. Because most people have several passwords they need to remember and it is never a good idea to use the same password on every system, there are even tips for making passwords easy to remember. One technique to create an easy to remember strong password is to use a pass-phrase. A pass-phrase is a technique in which you think of a phrase and then, pick all the first or last letters from each word and substitute some of the letters with numbers and symbols. You then apply capitals to some letters and substitute punctuation for others. Let's look at an example: taking the phrase "I will gladly pay you Tuesday for a hamburger today" we can turn it into iwgpytfaht or 1wgpyT4@ht. Using a password like this will make it easier for you to remember a long string of characters and it will make it much more difficult for a hacker to use a dictionary or brute-force password cracker to resolve the password quickly. Dictionary and brute-force password cracking tools are both freely available on the Internet. "An attacker will typically begin a password attack using the dictionary cracking tool" (Peltier et al. 2005). This isn't always successful, but a person using a six-character password with only dictionary words or numeric value-only passwords gives the attacker a limited list of possibilities. The dictionary cracker can run through the list in less than 1 minute. A brute-force password cracker takes a longer time because it has to run through every possible combination of characters until it succeeds. This means the longer and stronger the password, the more difficult it will be to crack. With a good password change policy in place, you will be changing your password before an attacker has a chance to break it.

Many organizations are enforcing strong, or stronger, passwords and most users therefore have at least one eight-character password to remember per system they need to access. Add that the user's passwords change every 30 to 90 days and it can become very cumbersome for a user to remember all of their passwords. For this reason, some organizations implement a technology called single sign-on to help with password management. Single sign-on allows each user to sign in once with one password and then the user will have access to all network resources. Although this technology is simple and convenient for the user, security professionals tend not to think highly of it because all it takes is for someone to compromise one password to obtain access to all network resources of a given user. Imagine what could happen if that user had elevated privileges or access to privileged information.

An alternative approach to the all-or-nothing single sign-on method is a technique called Common Credentials. Using Common Credentials, the user still only has to remember one user ID and password, so it can be a strong password, but rather than entering it once and having access to all network resources, the user will have to enter the password for each resource he or she wishes to access.

Institutions have been embracing a standards-based, open source technical solution for single sign-on called Shibboleth. "In addition to the SSO functionality, Shibboleth provides an attribute exchange framework with a strong focus on privacy protection. The identity provider, run by the user's home institution, uses the institution's identity management system so that attributes (e.g., the user's relationship with the institution) determine the user's access rights to the services. The service provider receives a set of attributes from the identity provider, agreed upon by the institution and the service provider, allowing him to make informed authorization decisions for individual access to the resources" (Oberknapp et al. 2009).

InCommon is the federation that exists to deploy the middleware, the software applications that can bridge network applications between institutions. This allows users to authenticate an application at another institution without having to have a separate account at that institution. InCommon provides a trusted framework for the use of authenticating technologies using Shibboleth as its technology. The technology connects the identity management systems between individual institutions (Mitrano 2006).

Both Common Credentials and InCommon are federated solutions and whichever authentication method is selected, password care and maintenance remains ultimately the responsibility of the user. Technology can protect systems but we must always educate users to protect their passwords and identities. The strongest password in the best protected system becomes useless if a user is careless enough to tell it to an airplane-full of strangers over the phone.

Unattended User Equipment

When we think about access control, most of the time, we think about system access and authentication. We need to remember that access control is also important in the physical environment. Have you ever thought about how much sensitive paper you've seen lying about the office in what many would like to think of as a "paperless society?" How easy is it for someone to pick up a laptop or USB stick and walk away with confidential information? It is important for organizations to have policies in place to cover these kinds of scenarios. Clean desk policies are intended to let users know it is their responsibility to make sure that when they are away from their desk, all sensitive papers are locked away and that they should use a password-protected screen saver to ensure nobody can access a system they are logged into. Policy can also be a good way to ensure that users secure their laptops with a locking cable when they are away and don't have their laptop with them. A thief looking for easy pickings will be looking for something that isn't locked down. Sensitive information stored on removable media should be required to be encrypted.

It is also a good idea to make sure printers, copiers, faxes, and scanners are in secure areas. For a long time, nobody gave them much consideration and now all it takes is the removal of the hard drive for an attacker to walk away with sensitive information. Do you have secure shredding bins in your office? Make sure they are emptied on a regular basis. There is nothing secure about a secure shredding bin that is full to the top. If someone can reach in and pull out the paper, it's too full. One of the things my current information security department does to assist community members is to hold ShredIT events. A heavy-duty secure shredding truck is brought on-site and the community is invited to bring any sensitive paper they may have to be shredded. These events are always well-attended and are often requested by the community. These events go a long way toward assisting the community with getting rid of sensitive paper. In a single year, more than 18 tons of hardcopy was shredded, some with PII dating back to 1865.

Network Access Control

With the volumes of information constantly moving across the network and the ever-changing way in which people use networks, making it more a part of daily life than ever before, the need for network security and network access control has never been more important. If you stop to think about it, our lives exist in cyberspace.

Security Components

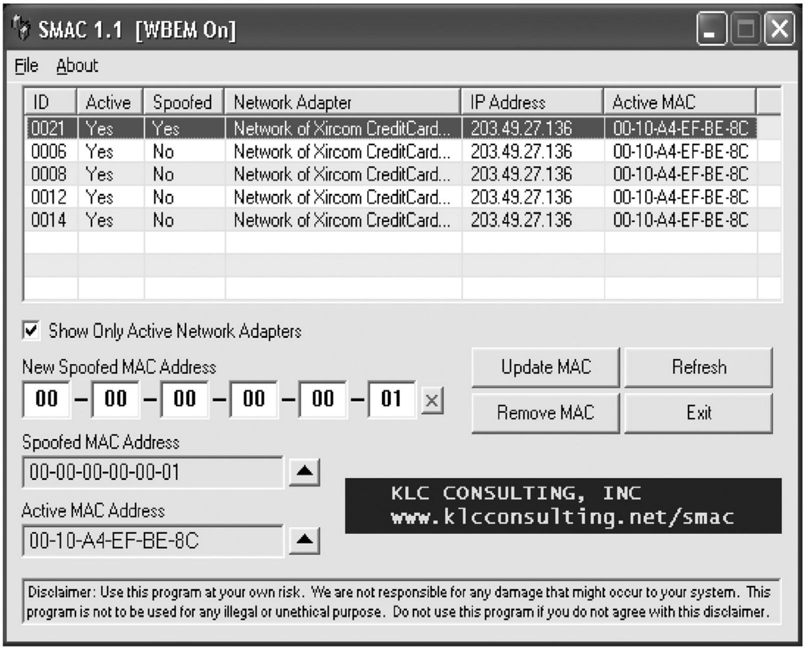
Protecting networking resources is one of the areas of information security that receives the most focus. When thinking of security, senior management often envisions firewalls, intrusion detection systems, and other technological solutions but often overlook the importance of integrating these with the existing user community. In this section, we will focus on the technical components of network security and how the technologies can be utilized to improve network security.

Many network devices are left in default or very similar to default configurations. Although leaving these devices in this state is often easier, it can be a severe detriment to security. Most devices in this configuration are running multiple unnecessary services and although these services are not directly used by the user community, the vulnerabilities in these services can be exploited by malicious users on the network. To minimize the amount of security holes in the network, the information security manager must disable or remove all the unnecessary services on the devices. This can quickly become a double-edged sword because determining which services are unnecessary can disable the functionality of the system. If you ever get a few spare minutes, look in the control panel on your Microsoft Windows system and see how many services are running on that system, but do not disable any services unless you know what the services do. It can be very easy to make a nonfunctional system this way.

Normally, a user with the appropriate access control is able to use any PC or workstation on the local area network to run an application or access certain data. However, where such data or system is classified as sensitive or requires restricted physical access, an enforced path may be applied. This is a straightforward configuration setting, performed by the information security manager, whereby access is restricted to a specific workstation or range of workstations. Enforcing the path will provide added security because it reduces the risk of unauthorized access, especially where such a workstation is itself within a secure zone, requiring physical access codes or other physical security mechanisms.

The typical network uses user authentication in which a user provides a username for identification and a password for authentication. In some networks, the authentication requires not just user authentication but node authentication as well. There are many different ways to get node authentication, it can be from a digital certificate issued to the machine, or based off of the system's IP address or from the system's hardware address itself. Using any of these authentication components with the user authentication component is not a good idea. With the exception of the digital certificate, it is very easy to change an IP address or hardware address to "spoof" an address of an authorized machine. By spoofing, the user on the rogue machine changes the system or IP address of the system to that of another system that is trusted or permitted on that network. The task of using hardware address node authentication was offered as a security solution for problems regarding wireless networks. This authentication was easily bypassed with spoofing, leading to the same security problems existing previously (Figure 9.2).

Another key component of network security is to have network monitoring in place. One of the easiest ways to securely monitor the network is to implement remote port protection. This would allow an information security manager to see if a new port becomes active on a switch or hub. A port is the term for one of the hardware interfaces on a hub or switch. Most hubs or switches are classified by the number of ports on them. You will often hear of 24 port switches, which means that there are 24 slots for network cables to be connected to the switch. In most



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0021	Yes	Yes	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0006	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0008	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0012	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0014	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C

☑ Show Only Active Network Adapters

New Spoofed MAC Address
00 – 00 – 00 – 00 – 00 – 01

Spoofed MAC Address
00-00-00-00-00-01

Active MAC Address
00-10-A4-EF-BE-8C

KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Figure 9.2 Spoofing hardware.

environments, there are ports that are not used and left open. If an attacker is able to get physical access to the switch, he or she can plug a new network device into the open port in the switch. Because this could lead to a security breach, the information security manager should be notified if one of these switch ports that have been unoccupied suddenly becomes active. This is where having remote port detection can provide security.

Yet another way to keep your network secure is to minimize the number of devices on a network that can be interacted with. To do this, the information security manager may choose to have network segregation. There are many mechanisms for achieving segregation in the network. These include using physical distance, virtual local area networks, network address translation, and routing. To use physical distance, the information security manager does not allow groups of network devices to be connected into the same hubs or switches as the other networks. This seems rather crude, but it can be quite effective. Imagine that on a multifloor building, the fourth floor is occupied by the Research and Development Department and no other user community needs to access this department. To stop other users from accessing this department, the information security manager can simply choose to not have the Research and Development Department share the hub or switch with the other networks. Although this method requires additional hardware, it is the easiest to manage. If additional hardware is not available, the information security manager may choose to perform the same segregation logically. To do this, the information security manager would use virtual local area networks. This allows one physical switch to be split into multiple logical switches. Although security using the virtual local area networks is not as good as the actual physical network, it can be quite good. The information security manager may choose to segregate the networks by using address translation and routing. In both of these examples, the information security manager will use different IP address ranges that have been administratively assigned to block communication between networks. The only real drawback to using this type of method for network segregation is if your organization uses a dynamic host configuration protocol (DHCP). If your network uses DHCP, a server will automatically assign IP addresses for all devices that are plugged into that network segment. A user can bypass the security of network address translation and routing by plugging the device into a new location and receive a new IP address.

Of course, one of the most often thought of mechanisms for getting network segregation is to use a firewall. Firewalls were originally an iron wall that protected train passengers from engine fires. These walls did not protect the engineer. This might be a lesson for information security managers. In early networks, a firewall was a device that protected a segment of a network from failures in other segments. However, the more modern firewall is a device that protects an internal network from malicious intruders on the outside. All firewalls use the concept of screening, which means that the firewall receives all the network traffic for a given network and it will inspect the traffic and either allow or deny the traffic based on the configuration rules on the firewall device itself. Many early firewalls would have a set of rules that would deny traffic that was not necessary for the business to function. Eventually, this migrated from a list of traffic to deny and accepting all other types of traffic, to a list of traffic to accept and denying all other types of traffic. This is often said to be a “deny all” unless it is expressly permitted type of firewall, which is currently the most common type. There are three primary types of technology that are currently being used: these are the packet filter, the stateful inspection, and the proxy-based firewall.

The packet filter firewall was the first firewall released and is often considered the simplest firewall. A packet filter firewall works off of a list of static rules and makes the determination based on the source IP address, destination IP address, source port, and the destination port. With a packet filter firewall, one of the common rules that need to be entered to permit the network to have web-based Internet access is a rule that allows all high ports (those above 1024) from all Internet sources into the organization. This allows any hosts on the Internet to send packets into the network over a high port and the firewall will permit it. This creates a rather large security hole into the organization.

The two second-generation firewalls, the stateful inspection and proxy-based firewalls, do not have this security hole. The stateful inspection firewall functions similarly to the packet filter firewall, but the stateful inspection firewall has a small database that allows for the dynamic creation of rules that allow for response traffic to enter back into the firewall. This allows for end users to still be able to visit web pages without creating the rule necessary for the response traffic to be allowed in. The stateful inspection firewall will dynamically allow the response traffic in if the traffic was permitted outbound.

The proxy-based firewall has nothing in common with the packet filter firewall. The proxy-based firewall actually functions by maintaining two separate conversations. One conversation occurs between the client and the proxy firewall, and the other conversation occurs between the destination server and the proxy firewall. The proxy firewall uses more of the IP packet to make the determination on whether or not to permit the traffic. This often causes some performance degradation, but can give increased security.

The information security manager often has to decide between easier administration and increased security. This is the case when it comes to control of the network routing. There are a number of routing protocols such as RIP, OSPF, and BGP that can be used. Anytime one of these routing protocols is used, it can make administration easier, but increases the security risk of having an intruder send false information over the router update protocol and corrupting the router's information table.

Cloud Computing

One of the current technologies being considered by organizations is that of storing information in the cloud. From an information security point of view, the issue here is that we don't know enough about cloud computing to understand how to properly secure it. The Cloud Security Alliance (CSA) was formed with the mission of promoting the use of security best practices in cloud computing and to promote a common level of understanding between consumers and providers of cloud computing with regard to necessary security requirements. A common understanding has not yet been reached. There are many issues to consider with cloud computing, such as where data will be stored and its legal ramifications. Does the cloud provider guarantee your critical information remains in the country if it is export controlled? Do they give assurances only appropriate users will have access to your data? Many organizations consider moving information to the cloud as a way to save money, as they are processing and storing so much data it is no longer economically feasible to own the resources the data lives on. They rent usage from the cloud provider and pay for only what they use and use is on-demand. A word of caution is necessary—organizations need to consider carefully what information they are moving to the cloud environment. Organizations should consider not moving critical information until they are certain that they understand exactly how and where it is being stored and how it is being secured. Organizations need to make sure what the provider is offering is what the organization intends. For example, an organization will certainly want to ensure that there is a clause in their contract allowing them to have access to the log records for a compromised account. As we navigate these waters, we need to ensure the access control decisions for our critical data remain with the organization and are not handed over to the provider without knowing exactly what is at stake.

Authentication

Authentication methods are important because this is the way users verify their identity to a system. For a long time, and in many cases still, the primary means of authenticating a user to a system was with a password. The password was intended to be known only to the user, and when the user entered it into the system, the system would then know the user was the person intended to access the information. It became evident in some cases that a password alone may not be enough, as users would write down their passwords and leave them in easy-to-find places or even share them. As previously discussed, weak passwords are also easily cracked.

Two-factor authentication is one of the methodologies being used by organizations for more sensitive systems and for users with higher privileged access. When you withdraw money from an ATM and have to present both an ATM card and a PIN, you are using two-factor authentication. Two-factor authentication takes advantage of multiple authentication technologies to provide stronger security by relying on two of three factors:

1. Something you know, such as a password or PIN
2. Something you have, such as a smart card, hardware token, or ATM card
3. Something you are, such as fingerprints, retinal scans, hand geometry, and palm prints

There is also a fourth category, which is something you do, that is sometimes added to this list. This fourth category would include things like keystroke patterns.

Category three, something you are, is in the field of biometrics. It is a field that is beginning to see more use, but has concerns associated with it. Biometrics is a field with great potential. More has probably been done with fingerprints than most other areas, but there are new things being done with biometrics all the time. One of the main concerns with biometric systems is the performance measures (Krutz and Vines 2003). The three main performance measures are

- False rejection rate (FRR)—this is the percentage of valid subjects that are falsely rejected
- False acceptance rate (FAR)—this is the percentage of invalid subjects that are falsely accepted
- Crossover error rate (CER)—this is the percentage in which the FRR equals the FAR

Most systems allow for an increase or decrease of sensitivity during the inspection process. The goal is to not set the sensitivity too high or too low, so the CER is used to obtain a valid measure of the system performance.

Enrollment time, or the time it takes to initially register with a system by providing samples of biometric information such as fingerprints, is another factor to consider. An acceptable enrollment time is approximately 2 minutes. Periodically, updates may be required for enrollment information. Over time, voices can change and fingers get cuts and scrapes that can change the surface features. "The stability of biometrics over time is an issue that affects biometric system performance. As people age, their biometrics change. Faces age, the skin on the fingers become less supple, and the ability to acquire fingerprints becomes harder. U.S. passports are reissued every 10 years, and the photographs on driver's licenses are required to be retaken every few years, depending on the laws of the local government. For biometrics systems to work with data from these documents, systems must be able to accurately compare biometric samples acquired at least 10 years apart. Longitudinal studies that assess how often a face, fingerprint, or iris biometric needs to be updated have yet to be conducted. The results of longitudinal studies will help determine which biometrics are appropriate for an application and how often an identity document needs to be updated" (Phillips 2009). The throughput rate, the rate at which the system authenticates individuals, should also be considered. Acceptable rates are an average of about 10 individuals per minute (Krutz and Vines 2003).

There are also potential legal, social, and privacy issues with biometrics. The biometric system used has to be accepted by the population that will use it. Although a significant portion of the population may have no objection to fingerprint scans, they may find retina scans more objectionable. If a retinal scan could potentially show health issues, what effect could that have on an employee and should an employer be able to use that information when it otherwise may not have been known? Securing the stored biometric information becomes very important. If a user's password is compromised, the user can call in to the help desk or use the organization's password self-service to obtain a password reset; but if an individual's biometric data is compromised, the individual can't have it reset.

There is a lot of research being done in the field of biometrics that will make biometric systems very adept authentication mechanisms. Information security professionals need to understand them and learn to correctly implement them.

Operating System Access Controls

There are a variety of access control methods appropriate for operating systems and policy should govern the methods that will be used in accordance with business objectives and the sensitivity of the information on the system. Logging should be enabled to record both successful and unsuccessful log-in attempts. Why would it be important to know about an unsuccessful log-in attempt? Does it really matter because they didn't get in anyway? Although it's true that unsuccessful log-in attempts may only be showing users who forgot their password on multiple tries, they may also be showing evidence of an attack. Wouldn't you like to see which accounts are being tried and when they were tried? The logs will show this. And if you have limited attempts enabled, you will be able to see if any of the accounts are maxed out. If the user hasn't requested assistance with getting back in the system, it's a pretty good bet the account was used in an attack attempt. The logs should also record when special system privileges are used. You could even go further and have a maximum number of log-in attempts set, so when that number is reached, a user can't even try to log in again without contacting an information security officer or help desk to have their account reinstated. This would then cause a conversation to determine if the user had, in fact, been the person to reach the limit in the number of maximum tries.

In some cases, for very sensitive systems, you may want to set automatic disconnect times. This forces the system to disconnect either when a user has been idle for a specified period or simply at a set timeframe. Setting automatic disconnect times forces the user to log back into the system and reauthenticate, and prevents someone else from logging in to an active session.

Another control that is strongly recommended is that each user should have a unique user ID for identification to the system. This user ID is for the use of the user only and, although it does not have to be private or confidential, used in conjunction with its authentication mechanism, it authoritatively identifies a user to a system. With proper logging in place, when a user ID takes an action in a system, it is documented by the system. If inappropriate activity has occurred using a specific user ID, there is no plausible deniability on the part of the person who owns the user ID. Sometimes, there will be requests for generic user IDs that are not tied to a specific person, but are used by a group of people. Use of these IDs is not recommended because there is no absolute way to determine which user was accessing the account when an action took place. If an organization does decide to allow the use of generic accounts, they should complete a risk acceptance form (RAF) so that senior management is aware of the decision. The RAF is signed by the business owner and documents the business reason for allowing the generic account along with the associated risk, and allows the requestor to ask that the risk be accepted by the organization. If approved, the RAF will also be signed by information security department which, in effect, agrees to share the risk. At no time should generic accounts be assigned to users accessing systems housing sensitive information.

Password security is an integral part of operating system access controls. One method users have long used for remembering passwords is to have two or three passwords they use in rotation so when they have to change their password they switch back and forth between the passwords. Another thing they will often do is use second passwords that are the same as the first and change only one character, usually something at the end. Systems should be configured in such a way as to disallow password reuse, at least for a set number of intervals. They should also be set to disallow similar passwords, so they will recognize when a new password is too close to the original. This control helps prevent a situation in which a current password may have been guessed or stolen and the new password is then easily inferred.

Teleworking

Through the years, IT workers have mostly been required to work in a cubicle at a desk in an office environment. Access control issues and standards mostly surrounded securing these in-office environments. Today's knowledge worker is looking for a new type of environment, one that is more flexible and doesn't require them to be in an office for the entire day or even every day. High gas prices, staying green, and overburdened highways are driving the need to work remotely and closer to or from home. Organizations are going to need to consider how they will handle the access control considerations because, to retain the best workers, they will need to adjust their concept of both a work environment and the tools that can be used within that work environment. For example, questions need to be asked surrounding the security concerns associated with using an Apple iPad for remotely accessing the organization's ERP system, and then decisions need to be made as to whether this type of access to organizational systems is appropriate.

Many of the access control methods already discussed also apply to teleworking. One of the most important things an organization can do is have a policy in place and make sure all employees who participate in teleworking are aware of the policy. Removable media and laptops should be encrypted and employees should be trained not to leave them unattended in vehicles.

With the right policies and adequate employee training in place, teleworking can be one of the best things an organization can do to improve morale and retain the best employees.

Summary

This chapter has discussed many access control methods, issues, and best practices. This has been done at a high level to give you a better understanding of why access control is so fundamental to information security. It's something we do every day without even thinking about it, but it's something we need to consider fully when our job is to protect the critical information of our organization and our clients. If we employ proper access controls, we are well on our way to doing our due diligence and providing a more secure environment in which to store our data.

References

Aldhizer, G.R., III. The insider threat. *Internal Auditor* 65, no. 2, 2008: 71–73.

Anderson, T. A cloud of suspicion hangs over online security. *IT Week*, July 21, 2008: 17.

Barcelo, Y. Beware. *CA Magazine*, September 2008: 36–43.

Bednarz, A. Should your IT staff telework? *Network World*, May 26, 2008: 23–24.

Bertino, E. Database security—concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing* 2, no. 1, 1 2005: 2.

Briguet, C. Building a secure collaborative infrastructure. *ECN: Electronic Component News*, February 2009: 27–29.

Cleary, B. How safe is your data? *Strategic Finance* 90, no. 4, October 2008: 33.

Collins, H. Security in the wireless world. *Government Technology* 21, no. 9, 2008: 44.

Communications News. Teleworking making strides. May 2008: 10.

Cornett, L., Grewal, K., Long, M., Millier, M., and Williams, S. Network security: challenges and solutions. *Intel Technology Journal* 13, no. 2, 2009: 112–129.

Galante, V. Practical role-based access control. *Information Security Journal: A Global Perspective* 18, no. 2, 2009: 64–73.

Grzybowski, D. Patient privacy: the right to know versus the need to access. *Health Management Technology* 26, no. 9, 2005: 54.

Helkala, K. Formalizing the ranking of authentication products. *Information Management and Computer Security* 17, no. 1, 2009: 30.

Hosseinzadeh, D. and Krishnan, S. Gaussian mixture modeling of keystroke patterns for biometric applications. *IEEE Journals* 38, no. 6, 2008: 816–826.

Information Security: GAO-08-526. Government Accountability Office, GAO, 2008.

ISO 27002:2005. ISO 27002_2005. *ISO 27002*, 06, 2005: 60–76.

Krutz, R.L. and Vines, R.D. *The CISSP Prep Guide.* Gold Edition, edited by Carol Long. Indianapolis: Wiley, 2003.

LeGrand, C. and Sarel, D. Database access, security, and auditing for PCI compliance. *EDPACS: The EDP Audit, Control and Security Newsletter* 37, no. 4/5, April/May 2008: 6–32.

Messmer, E. Telecommuting poses security risk. *Network World* 08, no. 04, 2008: 20.

Mitrano, T. InCommon: toward building a global university. *Educause Review* 41, no. 2, March/April 2006: 74–75.

Oberknapp, B., Ruppert, A., Borel, F., and Lienhard, J. From a pile of IP addresses to a clear authentication and authorization with Shibboleth. *Serials* 22, no. 1, 2009: 28–32.

Peltier, T.R., Peltier, J., and Blackley, J. *Information Security Fundamentals.* First. Auerbach, 2005.

Phillips, P. Biometric systems: the rubber meets the road. *Proceedings of the IEEE* 97, no. 5, 2009: 782.

Qingxiong, M., Johnston, A.C., and Pearson, J.M. Information security management objectives and practices: a parsimonious framework. *Information Management and Computer Security* 16, no. 3, 2008: 251–270.

Wiens, J. Guilty until proven innocent. *InformationWeek*, September 22, 2008: 50–52.

Chapter 10

Information System Development, Acquisition, and Maintenance

Quinn R. Shamblin

Contents

Information System Development, Acquisition, and Maintenance

Most organizations need information systems to varying degrees. Consumer product companies require the ability to process credit cards as just a normal part of doing business. Manufacturing and industrial firms use information systems to track, plan, and control their logistics. Educational institutions leverage information systems to automate certain classroom management and performance tracking tasks as well as many administrative functions. Not only are information systems used for the day-to-day process of business transaction and for business communications, but it is also often the information system itself that gives an organization its competitive edge (Ives and Learmonth 1984). Every industry has found areas in which operations have been enhanced or efficiencies improved by the deployment of information systems.

Planning

An organization planning to deploy or upgrade an information system will be faced with many decisions and activities as it moves through the life cycle of the system. This collection of activities is generally referred to as the systems (or software) development life cycle (SDLC):

- The business leaders will need to *plan* what they want the information system to do—to define the business goals that the system is to meet.

- Business and IT personnel together will need to *specify* the detailed functionality and features of the information system. What exactly will it do and how?
- The system will have to be *built* or *acquired.*
- It will have to be thoroughly *tested* by both technical and business personnel. Detailed communication between all affected levels, including support, will be required leading up to system *implementation.*
- Once up and running, the system will need to be *maintained* and kept up-to-date; changes must be understood and *controlled.*
- Finally, as the system reaches its end-of-life, plans must be in place for *retiring* or *replacing* the system.

Before beginning any information systems project, the business should understand that all these activities will be required to varying degrees and should be prepared to support them. There are a number of well-respected models to help an organization throughout the process, but regardless of the approach that is chosen, it is critical that information security be taken into account throughout the life cycle (ISO 2005).

ISO Controls Summary

Chapter 12 of ISO 27002, the Code of Practice for Information Security Management, covers the topic of information systems acquisition, development, and maintenance. Figure 10.1 shows the high-level control objectives.

Systems Development Life Cycle

One-time efforts are best managed using a formal project management methodology to ensure that important details such as scope, schedule, budget, adherence to specifications, suitability for use, and a host of other things are not missed. The best practice for managing an information systems project is a specialized version of project management referred to as a SDLC. There are several formal SDLCs that provide comprehensive guidance throughout the life cycle of a system or software package. Although they were not developed referencing it, the models generally fit very well into the project management processes proscribed by the Project Management Institute (PMI) and practiced by project management professionals.

Project Management as Defined by the PMI

This consists of five major project phases: initiation, planning, execution, control, and closeout (Project Management Institute 2000). Each phase of this framework incorporates a rigorous list of activities designed to ensure the successful completion of a given project. Figure 10.2 is provided to show a more complete scope of the activities included in the PMI framework (Mulcahy 2002, p. 24).

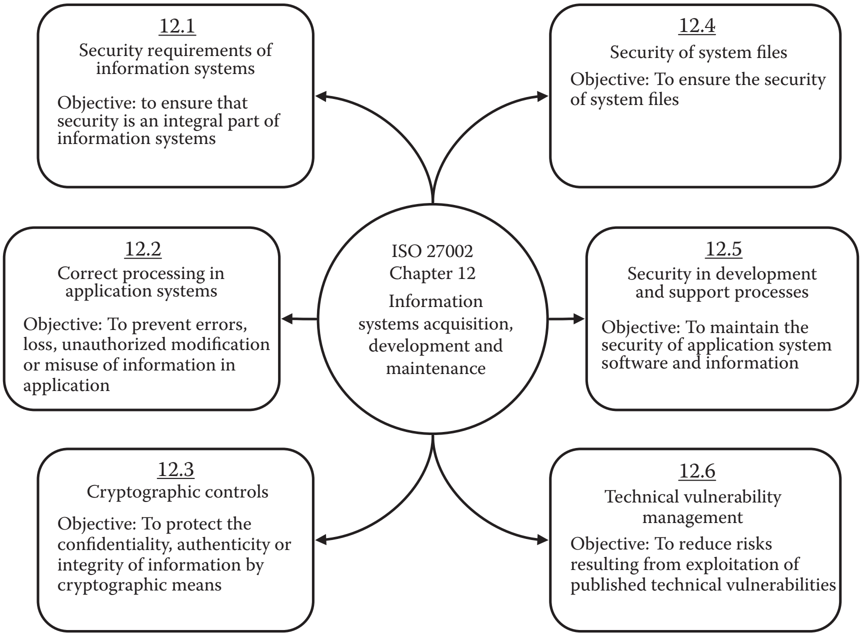

12.1
Security requirements of information systems
Objective: to ensure that security is an integral part of information systems
12.4
Security of system files
Objective: To ensure the security of system files
12.2
Correct processing in application systems
Objective: To prevent errors, loss, unauthorized modification or misuse of information in application
ISO 27002
Chapter 12
Information systems acquisition, development and maintenance
12.5
Security in development and support processes
Objective: To maintain the security of application system software and information
12.3
Cryptographic controls
Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means
12.6
Technical vulnerability management
Objective: To reduce risks resulting from exploitation of published technical vulnerabilities

Figure 10.1 High-level objectives of information systems acquisition, development, and maintenance as defined by ISO 27002:2005, Chapter 12 (ISO 2005).

If a certified project management professional is engaged, it is his or her responsibility to run a project with reference to this framework and to properly coordinate all phases. Projects run using this methodology have a much higher probability of successful completion: The end product or system is what the customer truly needs—no less, no more—delivered on time, within budget, and as smoothly as possible.

It can be argued, however, that not all efforts require the full rigor of the PMI framework. PMI concepts are often described by students of project management as a sort of formalized common sense. Therefore, although there exists no formal connection between the PMI framework and the various SDLC models developed separately, there are striking parallels between them. SDLC models incorporate many of the same concepts and activities of the PMI framework, but are often streamlined for the specific needs and challenges of a system or software development project.

In general, the benefit of these techniques is to ensure that the overall effort and all subparts are properly understood by all appropriate parties, that the process itself is transparent and accountable, and that the end product is fit for use. The scope of the work is defined in the planning stages (either all at the beginning or in the iterative phases) by gathering the input of all involved groups: the business, the development team, management, support personnel, the end user, etc.

Project Initiation	Project Planning	Project Execution	Project Control	Project Closeout
1 Business need 2 Project objectives 3 High-level constraints and assumptions 4 High-level deliverables and estimates ■ Base deliverables and time estimates or due dates ■ Deliverable alignment ■ Stakeholder list 5 High-level resource requirements 6 Project manager responsibilities 7 Project charter	1 Planning process 2 Scope statement 3 Initial project team 4 Create work breakdown structure (WBS) 5 Project execution team 6 WBS dictionary (including activity time and cost estimates) 7 Network diagram and critical path 8 Risk management plan 9 Develop calendar schedule 10 Develop project budget 11 Develop communications plan 12 Determine quality standards 13 Risk identification 14 Risk qualification and quantification 15 Risk response planning 16 Other management plans ■ Staffing ■ Procurement ■ Performance criteria ■ Reward system 17 Project control systems ■ Scope control ■ Work authorization system ■ Schedule control ■ Cost control ■ Quality control ■ Change control system ■ Dispute resolution 18 Formal approval and kickoff	1 Execute the project plan 2 Manage project progress 3 Complete work packages 4 Distribute information 5 Quality assurance 6 Team development 7 Hold progress meetings 8 Identify changes 9 Use work authorization system 10 Manage by exception to the project plan	1 Integrated change control 2 Project change control 3 Performance reporting 4 Scope verification and change control 5 Quality control 6 Risk monitoring and control 7 Schedule control 8 Cost control 9 Scope verification 10 Ensure compliance with plans 11 Project plan updates 12 Corrective action	1 Procurement audit 2 Product verification 3 Financial closure 4 Document lessons learned 5 Update records 6 End of project performance reporting 7 Formal acceptance 8 Project archives 9 Release resources

Figure 10.2 Detailed list of activities included in a project run using PMI methodology. (Taken from Mulcahy, R. *PMP Exam Prep.* 4th ed. RMC Publications, 2002.)

Knowledgeable representatives from each of these groups identify the needs. This approach allows for budgets to be aligned and resources to be allocated at the task level, a technique that produces much more accurate estimations if done correctly. Throughout the process, experienced resources are encouraged to provide systematic evaluation of risks and options to mitigate those risks. Finally, using an agreed upon framework allows for a shared vocabulary that is useful both within the team and in discussions with management and external groups.

SDLC Models

There are many well-respected SDLC models. Some of the more commonly used models are listed below, along with some of their advantages and disadvantages (Trompeter 2008). Different SDLCs address different needs, and they should be carefully evaluated before being applied to any specific project. Certified or experienced personnel should be engaged to manage the project and should be familiar with the chosen management model.

Sequential Models—This is a model in which each activity is fully completed, reviewed, and approved before the next activity begins.

Examples: Waterfall, dotted U, and V models (Figure 10.3).

Advantages: This is the most common approach and is simple to understand and manage. It is good for small projects or ones in which requirements are well understood.

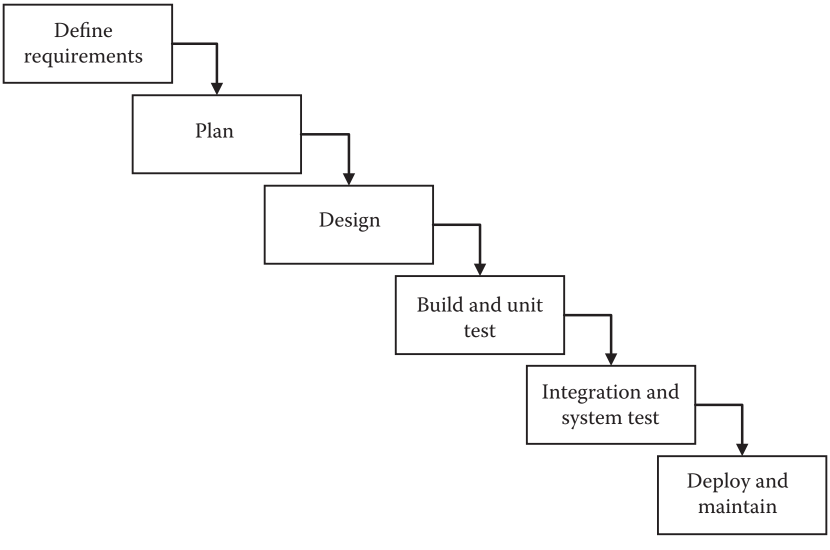


Figure 10.3 Basic SDLC waterfall model.

Disadvantages: This approach is very rigid. If the project is long, complex, contains uncertainty, or may need a change in scope after a portion of the work is already complete, then this model is not a good choice. No results are produced or testable until late in the life cycle.

Iterative or Incremental Models—This could be thought of as a more intuitive and flexible version of the waterfall model—a “multiwaterfall” model. It focuses on the early delivery and testing of small portions of the project to allow problems to be uncovered early, and then builds on the corrected version for later iterations. If any issues are uncovered in the testing of the smaller parts, the process restarts for that element.

Examples: Rapid Application Development (RAD) and Rational Unified Process (RUP; Figure 10.4).

Advantages: This method generates a working system—albeit with only limited features and functionality—quickly and early in the process. It is thus more flexible and less risky than the strict waterfall model; it is easier to test and less costly to correct as this may be handled during each smaller iteration.

Disadvantages: Each individual integration (often referred to as a “phase”) is rigid. This model mitigates some weaknesses of purely sequential models, but still does not completely resolve the issue that system architecture or design problems can be costly to correct if all requirements are not identified early enough.

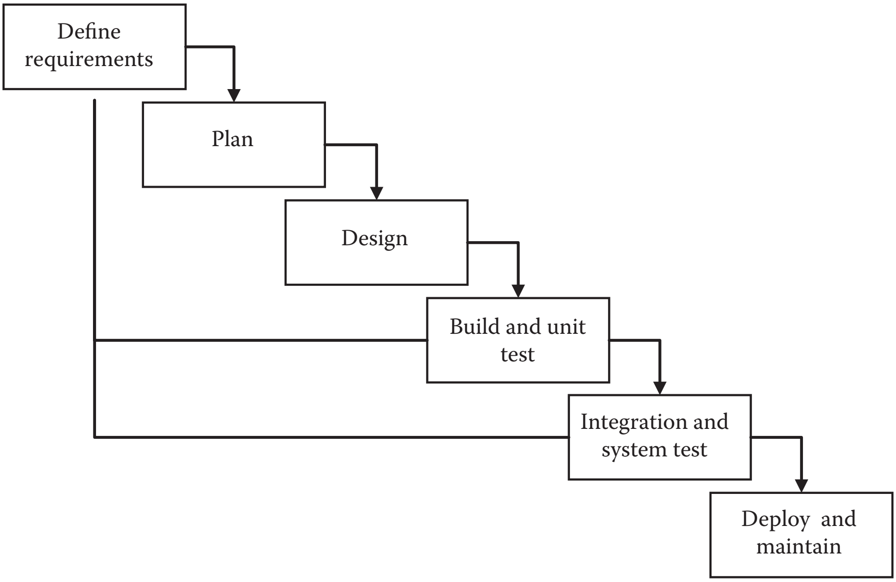


Figure 10.4 Iterative SDLC model.

Evolutionary or Prototyping Models—In this model, developers build functional versions of the system and work with customers to test and learn what works and what does not. Gradually, they build better and better versions, evolving to the final design (Figure 10.5).

Examples: Adaptive Software Development (ASD), Spiral.

Advantages: More time and effort is spent on risk analysis, leading to better risk management. A working system or software product is produced early and often, is evaluated by the customer, and improved based on direct customer feedback to the project team. This is good for large or mission-critical projects.

Disadvantages: This model is costly. The total cost of the project is the sum of all required phases. The project is dependent on solid risk analysis, which requires highly specific expertise. It is not a good choice for small projects with more limited budgets.

Agile Models—These models are based on a philosophy published in 2001 under the name Agile Manifesto, the core of which is shown in the callout box (Beck et al. 2001). Agile methods focus on meeting the needs of the user more quickly and with less cost, by including both business analysts and developers in the teams and workshops where needs are defined. The approach may be feature driven, use case-driven, model-driven, test-driven, etc., but the applications are delivered incrementally. A small set of features is defined and designed in face-to-face collaboration with the users, is created and delivered in a short time frame, and is tested, accepted, and put into production. Then,

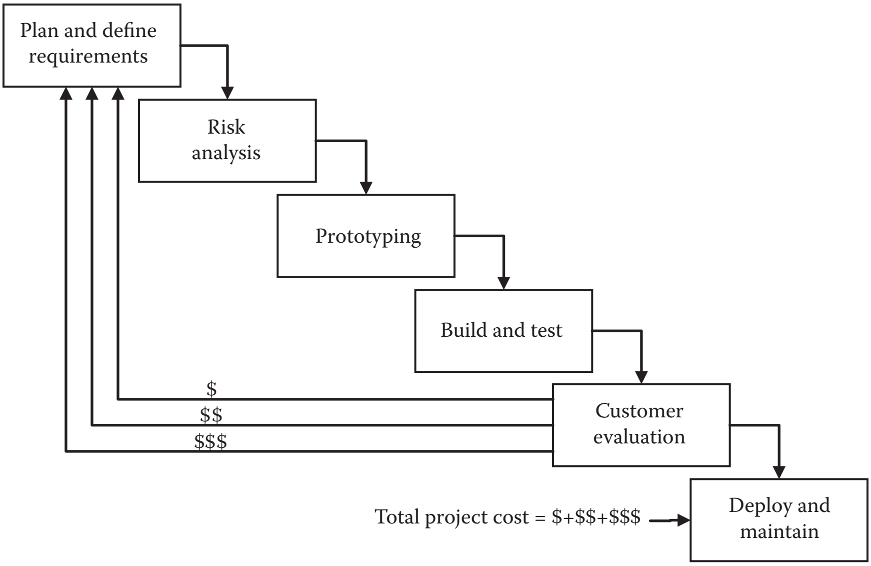


Figure 10.5 Adaptive Software Development (ASD), Spiral.

MANIFESTO FOR AGILE SOFTWARE DEVELOPMENT

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

That is, while there is value in the items on the right, we value the items on the left more.

the next iteration starts, with each iteration getting closer to the end vision of the product and each providing a useful output along the way (Figure 10.6).

Examples: eXtreme Programming (XP), Agile Unified Process (AUP).

Advantages: This is a people-focused model. There only a few rules and best practices and these are easy to employ. This is a good model to quickly produce partial solutions. It works well in environments that change steadily and supports concurrent development within an overall planned context. It can improve teamwork, motivate, and cross-train.

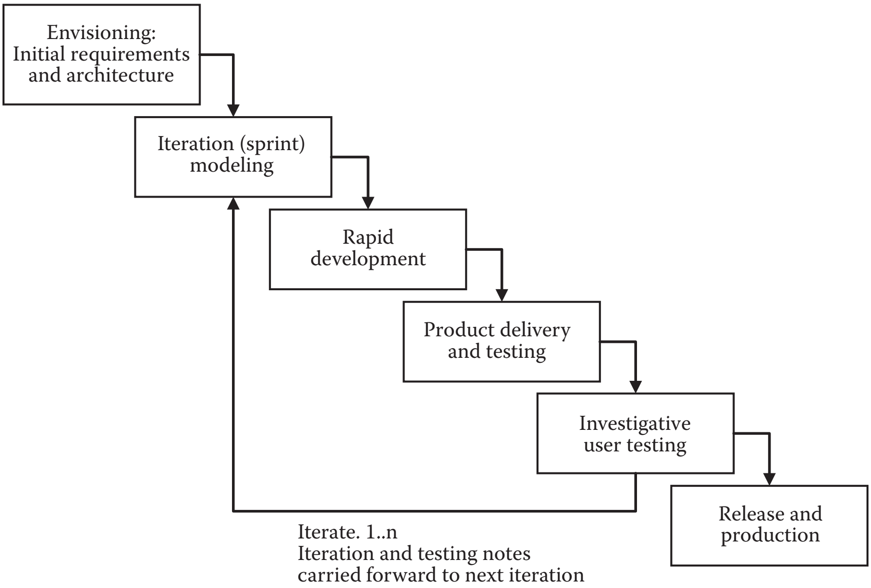


Figure 10.6 eXtreme Programming (XP) and Agile Unified Process (AUP).

Disadvantages: The Agile model is managed by a strict delivery methodology, which dictates the scope, functionality to be delivered, and adjustments to meet the deadlines. This model will not help drive culture change (poor communications, prima donnas, or micromanagement) and can be seriously affected by these issues. It does not work without an overall plan, an Agile leader, and Agile PM practices.

Of the various types of models, Agile models are currently the most popular for large and detailed projects. Sequential models require the most written documentation, but rely the least on graphical models and in-process customer interaction and thus tend to incorporate greater risk and be more prone to delays.

Although one framework may be desirable over another from the point of view of project management needs, the specific framework chosen makes little difference from a security standpoint. It is more important that there *be* a framework, than it is that a certain framework be selected. When there is a structured approach to managing the project, security can be more smoothly and systemically inserted into the process. Every project requires consideration of many security elements, and a formal process for project management, with agreed-upon stages or phases, helps guide the project team through these considerations and ensure that these critical elements are properly included.

Some Types of Application Technologies

One important element to planning a new system is the selection of the technology to be used. Often, the selection is made based on what the organization is most familiar with. However, care should be taken with the selection of the technology because each has its own security considerations and challenges.

Web Applications

Applications can be built to run through a web browser over the Internet or internal network of an organization. Some of the coding languages and standards that are commonly used for this are html, Java, C, C++, PHP, JavaScript, Python, C#, Structure Query Language (SQL), Perl, Ruby, Shell, Visual Basic, .net, JSP, ASP, flash, and many others.

Creating a web application that both fulfills the functional needs of the customer and provides proper security for the associated information requires careful thought and planning. There are many, many attacks that can be made against a web application—enough to fill several books all on their own—but here is a short summary of a few common types of attack:

- *Denial-of-Service (DoS) Attack*—An attack wherein the attacker sends a flood of requests to the server in the hope of exhausting all system resources, such as available ports, memory, or processor capacity.

- *Distributed Denial-of-Service (DDoS) Attack*—A type of DoS attack in which the attacker installs a control program on multiple computers. The attacker can command all systems under his or her control to attack. DDoS is more effective than DoS because the number of attacking machines is limited only by how many computers the hacker can get under his or her control. Malware is often used to infect machines without the knowledge of the owner. DDoS is also more difficult to stop because blocking a single IP address or network range will not stop systems on other networks.
- *Code Injection*—A class of techniques in which an attacker introduces or "injects" code into a computer program to change how the program runs. This is commonly used to bypass security protocols and can be one of the more serious types of attack.
- *Cross-Site Scripting (XSS)*—A type of code injection in which attackers inject client-side script into web pages viewed by other users. This attack exploits the trust a user has for a particular site and is often accomplished by crafting a malicious URL that directs a user to log into a malicious site while thinking it is a trusted site.
- *Cross-Site Request Forgery (XSRF or CSRF or Sea-Surf)*—A type of code injection in which unauthorized commands are transmitted from a user that the web site trusts. This is often done by stealing information from a victim's cookie or session and using that information to trick a web site into thinking that the attacker is someone that the site trusts. This attack is the opposite of XSS in that it exploits the trust that a site has in a user's browser.
- *SQL Injection*—A type of code injection that exploits a vulnerability in the call that a web page makes to a database. When user input is not correctly sanitized, an attacker can run any SQL statement he or she may choose and can extract unauthorized information from the database or even destroy it. SQL injections will be further explored later in this chapter.
- *Session Hijacking*—An attacker steals a valid computer session to gain unauthorized access to information or services. Often, the cookies that web sites use to maintain a session can be easily stolen by an attacker using a computer somewhere on the network between the client and server. Another form is TCP session hijacking, wherein a hacker takes over a TCP session between two machines after an authorized user has successfully authenticated, something that usually happens only once, when the session is first established. After the session is hijacked, the attacker has access to the compromised system just as if they were the person from which the session was stolen.

This list is not all-inclusive and more attacks are being developed continually. Application developers should keep up to date with the various types of attacks and understand how to write code to defend against them.

Object-Oriented Programming

Object-oriented programming (OOP) is a type of programming language in which the developer builds distinct "objects" or "classes" that define not only the types of data and their structure but also the specific functions or "methods" that may be applied to that data. Each object contains its own method(s) and data structures. Applications and computer programs are then built using these predefined objects. This is distinct from "procedural" languages, which organize programs in terms of variables and function calls or subroutines. A few well-known object-oriented languages are Java, C++, C#, .NET, Smalltalk, Python, Ruby, Jade, and more (although some of these are not purely object-oriented and also include some procedural elements).

One of the security challenges of programming in general is to instill in developers an understanding of the importance of security. Focus is often on functionality and security is left as a last consideration, if included at all. In the modern world, this can no longer be allowed. Programs and systems are under attack all the time and those that are not written to be secure, will be compromised.

Object-oriented program languages can offer an important security benefit, however. Each element of the desired system can be written so that the features and functionality that it provides overlap as little as possible with other elements. This is referred to as "separation of concern" and is an important consideration in the design and architecture phase of a solution. By controlling which methods have access to what specific data or can take which specific actions, *and* by ensuring that no other method can do so, the system can enforce security much more effectively.

The development community is growing to be much more security-conscious. It is an embarrassment to the organization and to the profession when a system is compromised. There are many excellent development frameworks that are well tested and effective from a security standpoint. Security-conscious organizations will ensure that their development teams are using such frameworks and are engaged with the development community for whatever platform they are using, monitoring them for the latest information on security issues. One excellent resource for this kind of information is OWASP (http://www.owasp.org).

Services-Oriented Architecture/Web Services

A services-oriented architecture (SOA) provides a loosely integrated suite of "services" that are available to applications within a business' domain. Each of these services can be thought of as a function or method that is available on the network and may be called by any system with proper authorization.

For example, an insurance organization may have a suite of services that provide the functionality required by their organization. There may be a single service that provides the full details of client contact information if the client's name or phone number is provided. Another may list all details of a policy when provided a policy number. Another may provide a list of all claim numbers made under a specific policy, etc. Each of these services could be written so that they supported both a read and a write function, or separate services could be created for each of these purposes.

One important benefit of this architecture is that the user interface, for example, a web-based portal, is separate from the systems that actually hold the data. The back-end databases and data processing servers may only be accessed through the services and those services can be written to provide rigid security and to expose only the specific information required. This can be a great benefit to security.

Another strong benefit is that services can be written to enforce separation of concern, meaning that there is one web service—and only one—that is permitted to access a given type of information. The code for each service can be made very secure while at the same time allowing for smooth delivery of all business needs.

Again, one challenge is to ensure that security is incorporated beginning with the initial design phase. If a web service will provide sensitive data, it must have some method to ensure that the only applications that can access it are authorized to do so. This is often done through certificates, credentials, or access control lists, among other techniques.

Database Systems

Data from all types is most often organized and stored in some form of database. Databases allow for large amounts of information to be stored more efficiently and to be accessible very quickly.

One way they store information more efficiently is through a process of "normalization." That is, the data is structured so that information that is the same for many records is only actually written into the database once and is referenced when needed.

To get an idea of how this works and how it can be a real space saver, consider a company that sells books. Each book has a number of different qualities that are important: title, author, price, description, format, weight, ISBN, and many more fields; perhaps even information such as customer rating, awards it may have won, etc. Suppose a customer puts in an order for three books. Instead of copying all or some of these important pieces of information into a table under the customer's name, in a relational database all that has to be included in the order table is a unique identifier for that particular book and how many have been ordered (an item's unique identifier is also called a primary key and may be an item number, SKU, ISBN or something similar). All the rest of the information can be kept in a "products" table and referenced by the primary key only when actually needed. If 10,000 people buy a copy of a book, the database does not have 10,000 copies of that book's title, price, etc., but just the primary key pointing to the book's record.

Data is usually extracted from relational databases using SQL. This language allows developers to write a request for data from the database in a form that is easy to understand. For example:

```
select * from table “customers” where lastname=“Washington”
and firstname=“George”;
```

The above SQL query would return all the data in the customer table for the record that has the last name of Washington and the first name of George. However, if applications that use SQL are not properly coded to protect against it, they may be vulnerable to an “SQL injection” attack. In this type of attack, a malicious user enters a value containing special characters designed to disrupt the normal action of the query. For example, in the query above, a malicious user might enter the following when asked for their last name:

```
*”;–
```

If the application is not coded properly, this value will be inserted directly into the query to look like this:

```
select * from table “customers” where lastname=“*”;–  ” and
firstname=“George”;
```

The “–” characters tell SQL that everything after them is a comment, so that part of the query is ignored and the effect is this:

```
select * from table “customers” where lastname=“*”;
```

The above “hacked” version of the SQL query would return all the data in the customer table for *all* records. This would allow an attacker to extract the data from the entire customer table.

Proper coding techniques can prevent this sort of attack. The application should be written to not allow certain characters like*— ( ) # ; and a few others. The application should also check that the input is what is expected. If a number is expected and someone puts in a text value, the code should properly handle that error. If a field is expecting letters, apostrophes, single dashes, and periods only (as would be the case for a name field), the code should detect and properly handle any nonpermitted characters. There are several other techniques that should be employed to protect these types of applications against SQL injection. References are readily available that provide more detail on this topic.

Requirements

Different SDLCs suggest different methods to gather requirements for the project. Sequential methods, such as Waterfall, have the requirements for the final product documented in full before any development work begins. A complete description must be provided including the functional requirements (behavior or use cases) of the system and the nonfunctional (supplementary) requirements that influence or constrain the design or implementation (budget, performance, quality standards, technological, design, or other constraints). On the other hand, Agile methods require just enough requirement information to drive the next iteration or sprint. There exists a great deal of material on how to develop requirements for a project, so there is no need to go through those details here; however, it is extremely important that security considerations and concerns be addressed during the requirements phase or phases in whatever form they may take. As the application's features are determined, they should be reviewed to determine if there are security implications to those features and what additional requirements should be added to address those implications.

For example, if a bank is writing an application to allow customers to do their banking online, one of the requirements better be that the connection between the user's computer browser and the bank's server *must* be encrypted. But even more than that, it must be encrypted using an approach that is at or above the level of the current industry standards for such encryption. If an encrypted connection cannot be established, the server must reject the connection attempt.

Another requirement might be that the system not only asks the customer for their username and password but also that the password is required to be a strong password. A fun fact: If a password is any word out of any printed dictionary on the planet, a hacker using modern password cracking methods can break your password in less than 10 seconds (approximately, depending on a lot of technical details). Alternatively, a password that includes all four elements of a strong password—uppercase and lowercase letters, numbers, and symbols—and is eight characters or more, may take centuries of computer time to break.

Each specific type of project has its own concerns and its own unique elements that require security considerations. A database containing social security numbers might be configured to reject all attempts to connect to it unless the connection includes a special strong password *and* comes from a particular IP address. A system containing critical information on a new product expected to bring in a billion dollars' worth of business may be protected not only by a password, but also an ever-changing code number on a token carried only by authorized users (this is known as two-factor identification, described in the chapter on access control).

> *From the Standard (ISO 27002:2005)*: Automated and manual security control requirements should be analyzed and fully identified during the requirements stage of the systems development or acquisition process, and incorporated into business cases. [12.1 Security requirements of information systems] (ISO 2005).

Once the functional specifications are completed and reviewed for security concerns, it is time to consider the process of development itself. Development should always be done using coding frameworks that have been tested and are well respected by industry security experts. Coding should be managed with strict reference to best practices. Building these elements into the documented requirements for the project is a good start in helping guide it in the right direction from a security perspective, but this alone is not enough. The functional requirements themselves need to plan for security. Another consideration is one of vulnerability testing. Security reviews and testing (discussed later) should be built into the requirements. This can give management a stronger degree of confidence that they are doing their due diligence.

Throughout the remainder of this chapter (and indeed throughout the book) are many items that can be considered and may be included in the requirements of an application. Doing so will make it clear that security is an important element of the project and must be integrated into the application at the deepest levels.

> We need secure products, not security products.
>
> **—Phil Venables**
> *CISO, Goldman Sachs*

Specifying

Through the requirements phase, the business has supplied its requirements for the application or system. It is now up to the project team and other appropriate stakeholders to determine how those requirements are to be met. If the project is to be developed using outside resources, a nondisclosure agreement should be drawn up and executed before sensitive business information is shared with the external agency.

Security must be considered throughout the development of the system architecture and design. Some common areas where security controls should be considered are

- *Operating Environment*—How will the operating environment be set up to support the required level of security for the application? An application cannot be secure if the server or network on which it is running is not secure.

From the Standard: Access to system files (both executable programs and source code) and test data should be controlled. [12.4 Security of system files] (ISO 2005).

How is the network protected? Who has access to the domain controllers? Who has authority to create or assign group policies? Who will be allowed to log into the server as an administrator? As a user? Will shared accounts be allowed? (In the author's opinion, the answer should be NO!) Will security logging be activated? Will activity logging be activated? How long will the logs be kept?

- *Access Controls*—Is the application meant to be accessible to anyone? If not, how will it *ensure* that *only* an authorized person is allowed access? Beyond a user name and password, what controls can be included? For example, if the only people that are ever supposed to access this application are supposed to be doing so from within the company's network, the server can be set up to *only* accept connections from an internal IP address. Will the system not only require the user to authenticate him or herself (by providing a username and password) but *also* authenticate itself to the user (by showing the user a picture and/or phrase selected by that user during account setup)? Is it permissible for the system administration group to have a single administrative password that they all share, or will each administrator be required to have credentials (username and password) unique to them?
- *Data Type*—Will the system deal with sensitive or regulated data (financial, medical, personal, etc.)? If so, are there any special requirements or considerations when dealing with that type of data?
- *Data Validation*—Will the system accept input from the user? If so, how will the system ensure that the input is valid and correct and will not cause the system to behave in an undesired way? For example, SQL injection attacks are still happening today. These attacks often hinge on a malicious user entering special characters like quotes ('), equals (=), wildcards (? or *), or escape characters (—) into a user name or password field. These special characters can cause poorly written database code to be completely co-opted and provide the cyber criminal access to data throughout the victim database. A very effective solution is to "sanitize" the inputs, make sure they are the correct data type and do not contain characters that have no business being there. There are other mitigations that should also be employed, but these will not be discussed here.
- *Data Protection*—How will the data be protected when at rest (on a hard drive, for example)? Will it be encrypted? Will the server be set up to have tightly-monitored access control lists (ACLs)? Will access attempts be logged? Monitored by automated systems? Audited? How will it be protected when in motion (moving across the network or internet)? Will the system require an encrypted connection before it allows a user to authenticate?
- *Request/Message Validation*—What processes will be in place on the server to ensure that a request is valid? How will the server tell that a request for

processing that is otherwise properly formed and free from error comes from an authorized source? Will it be able to detect a problem if requests are supposed to only be for a single record and suddenly it sees a request that will return more than one record?

- *Transaction Records and System Activity Logging*—Does the system provide facilities to ensure that a person cannot claim that they did not make the connection or that they did not receive the information (nonrepudiation)? Is a digital certificate being required and used? Are IP addresses, dates and times being recorded for activities in the system?
- *System Response Validation*—Similarly, will the client system be able to detect an anomaly? Will either the server or the client be capable of automated action in such an event? What can or must be done manually?
- *Incident Handling*—In the event that an anomaly occurs and cannot be stopped or corrected by automated means, what will the system do? Will it provide a real-time alert to Support and/or Incident Response personnel? Is the system equipped to help such personnel understand what took place and take appropriate action? Are logs being kept?
- *Data Retention*—How long must the data be kept? How is it to be handled when the data retention period is over?
- *Business Continuity and DR*—How long can the business go without this application and/or the associated data? If the system goes down, how long can it be down before it affects the business? What steps will be taken in this event to allow the business to continue without the system? In the event of a disaster, how will service be restored? What steps are involved? How long will it take? If the business will be affected before service can be restored, what can be done to shorten the recovery time? What will it cost to meet the shorter time?

There are a lot of questions here, and this list is by no means all-inclusive. There are more questions and each of these questions often lead to more questions, and every question may be answered in many different ways. Experienced and knowledgeable people must be engaged throughout the architecture and design phases to make sure these questions are asked and, more importantly, answered in such a way as to meet the needs of the business while ensuring that the confidentiality, integrity, and availability of the information is maintained.

> Ultimately, it's up to all of us…to stop designing insecure systems. It is as simple as that.

—Paul Simmonds
Global Information Security Director for British
conglomerate ICI Plc., and cofounder of the Jericho Forum,
during his keynote speech at Black Hat Briefings, 2004

Protecting Sensitive Data Types

It is particularly important that any data categorized as sensitive or protected by regulation is properly protected. This raises the questions: Does the organization know what data it has, if there are regulatory requirements surrounding that data, and where the data is located? It is not at all uncommon for workers—in an attempt to make the fulfillment of their duties easier or faster—to create spreadsheets or private databases containing frightening amounts of regulated data. Are these databases stored on a centrally managed server and well protected or are they on the person's laptop or USB drive? Has an employee ever e-mailed a document containing sensitive information to their home e-mail address? If so, was a copy of that e-mail also sent to their mobile phone? Is the mobile phone encrypted and password protected?

It is critical that management pass policies on data classification and data protection. Members of the organization need guidance on what must be protected and how. Once the organization knows what data it has and where it is located, it is in a much better position to design protections.

Data protection is usually designed using layers. Each layer provides protection against several types or classes of vulnerability and, although each is insufficient by itself, taken together, they present very strong protection. This approach is often referred to as defense-in-depth, and is shown in Figure 10.7. As the shade in this depiction gets darker, the area is more and more protected.

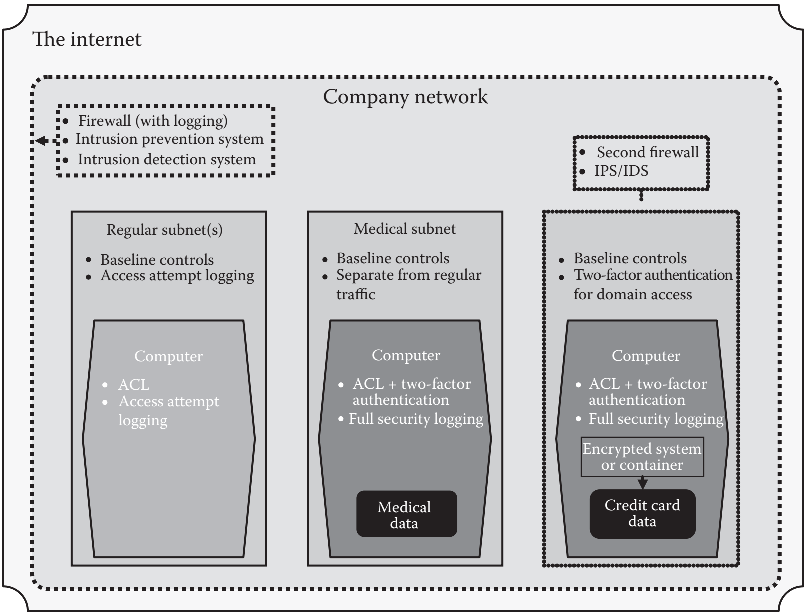


Figure 10.7 Defense-in-depth.

> *From the Standard*: A cryptography policy should be defined, covering roles and responsibilities, digital signatures, nonrepudiation, management of keys and digital certificates, etc. [12.3 Cryptographic controls] (ISO 2005).

For highly sensitive data such as social security numbers (SSNs), financial data, credit card numbers, medical records, etc., strong protection techniques should be employed, especially if that information is going to be stored on any type of portable device like a laptop, USB drive, mobile phone, etc.

Think about smart phones. These phones are designed to allow users the same functionality as a computer—including e-mail. If a person e-mails a file to a colleague and that file contains sensitive data, a copy of that data is now present on that phone. What happens if that phone is now lost or stolen? You have a data breach. Most states in the United States have data breach notification laws. When protected data is compromised, the organization responsible must notify the affected persons and sometimes—depending on the details—the media, the attorney general's office, etc. However, most of these breach notification laws include language that excludes encrypted data from these requirements.

Consider this scenario: a person is e-mailed a spreadsheet containing 10,000 names and social security numbers. They are on the road and so they open the file to ensure that it is what they need when they get back to the office. Unfortunately, on the way to the office, they stop for coffee somewhere, put down their phone and forget it. By the time they go back to look for it, the phone is nowhere to be found. If that phone is encrypted and has an access password, or better yet, if the spreadsheet file itself is encrypted (modern office software natively includes options allowing for the strong encryption of files), *there has not actually been a data breach*. The only effect on the company is that it must buy a new phone. If, however, the phone is not encrypted and does not have an access password and the file is not encrypted, the company *does* have a data breach and is required by law to report that breach. According to research done by the Ponemon Institute on behalf of the PGP Corporation, the average cost to a U.S. company of each record lost in a data breach was more than $200 in 2009 (Ponemon Institute 2009). That $200 includes the costs of the notification, lost business, reputation damage, and other effects. That means that this stolen cell phone has just cost the company two million dollars ($200 × 10,000 records = $2,000,000). Two million dollars lost because someone e-mailed a document that was not secure, in an insecure way, and that document was present on a smart phone when it was stolen. It is critical to develop policies on data protection and make sure that all employees who work with or may come in contact with sensitive data understand those policies.

From the Standard: Data entry, processing and output validation controls and message authentication should be provided to mitigate the associated integrity risks. [12.2 Correct processing in application systems] (ISO 2005).

Data Validation

An application that works with data in any fashion must provide facilities to ensure that the data it receives, processes, returns, and displays is correct.

This is a highly detailed topic with many possible methods to ensure the integrity of the data and the system. Many of the questions included in the section above on specifying will help the project team to more fully flesh out how to handle this area. If the data being collected in a web-based form is not properly handled, it could allow a hacker to read your entire database or even destroy it. Similarly, if the server does not validate that the request is of the correct form and from the correct source, information can be stolen by unauthorized people.

It is, however, important to recognize that not all applications and not all data require the same level of protection. Providing the highest level of protection to all data and all systems in the company may cost the company more money than it needs to spend. This comes back to the data classification and data protection policies.

An application that does not deal with sensitive data, for example, a mobile phone application that allows students to check when the next shuttle bus to the other side of campus is due to arrive, does not need the heavy protection required by a student information system containing course schedules and grades. The information in the student information system is protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), whereas the information on shuttle bus movements is posted publicly on a sign next to the bus stop anyway.

This is where risk analysis and security reviews come into the picture.

Threat and Risk Analysis

Whenever a new system is being designed or if a major change is being planned to an existing system, a security review of the proposed system requirements and architecture should be conducted. This is especially important if the system deals with any sensitive data.

A cyber criminal who can subvert the function of an application or can get control of the server on which that application runs will be thrilled just to have those extra resources at his or her command, but the implications of a compromise of an application that deals with sensitive data can be truly frightening. If an online banking application is not secure, criminals are going to exploit it as much as possible—steal as much as possible—until the application is taken offline or secured. The bank will face Federal fines, loss of customer confidence, and more. If the breach is large enough or the bank small enough, it is not unreasonable to imagine the future of that bank might be in jeopardy.

A security review will give the organization a much higher degree of confidence that the final solution will be one that can be trusted. Corporate officers have a duty of due diligence and these reviews are part of that due diligence. A security review involves the consideration of a wide array of threats and evaluating the risks associated with those threats. The review may uncover weaknesses that were not originally considered by the business and may require modifications to the solution architecture. Many people are concerned that security will slow them down or stop them from doing interesting things—that security is going to always say "no"—but in reality, the point of the security review is not to say "no," but rather, to find a responsible way to say "yes." Uncovering a security vulnerability does not necessarily mean that the project cannot move forward; rather, it means that some form of mitigation or compensating control needs to be included so that the project can move forward without exposing the organization to undue risk.

The review does not necessarily need to be conducted by an external person or agency. It may be desirable to bring in experts if designing a solution of extreme sensitivity or one in which the organization does not have a great deal of experience. However, it is often the case that the organization has (or can develop) the skill to do such reviews in-house. One thing that must be borne in mind however is that the person doing the security review should not be the same person who is designing or developing the solution. The reviewer must be responsible for security—to have security as a primary job function—with an organizational driver motivating that person to really dig into the security of the proposal. It is rare that a developer or manager of a development team is a good fit for this type of role because their motivators will be in conflict. They will be under deadline pressure or under pressure to include features or functionalities that are not yet ready for production. These considerations can run counter to good security. Having a different person designing and testing the controls is also important from the perspective of separation of duties. Just as with writing, the person doing the editing should not be the original author. A second set of eyes will see things to which the first is blind.

Building/Acquiring

The project team now knows what it is they are to achieve (requirements phase) and they have worked out the details on how it is to be done (specification phase). Now it is time to actually buy the solution if one already exists or build it if it does not (or if the financial picture of that option is more attractive). Systems can be acquired from a variety of sources, including as off-the-shelf software or hardware packages, as the work product of consultants or vendors, or as a hardware appliance or software as a service (SAAS) solutions that reside in the cloud. Alternatively, an organization with the required technical resources and expertise in-house may elect to build the system.

This issue of source is important:

- Is this going to be an off-the-shelf solution purchased from an outside vendor? If so, is it a turnkey solution that requires nothing more than a basic installation or does the solution require special expertise to deploy? If so, will professional services be required or can in-house personnel handle them? Will special training be required?
- If the solution is going to be built, is it going to be developed by a vendor, a consulting group, or an in-house team? Depending on which is chosen, different resources will be available and different costs incurred.

Vendor-supplied solutions may have a heavier upfront price tag; however, if a solution exists, it is often worth considering. Such a solution may incorporate elements or features that the business or project team did not think about during requirement/specification, but that are important nonetheless. Vendor-supplied solutions are more likely to be kept up-to-date, an important consideration from a security perspective. They are also more likely to have access to greater security testing resources: rigorous cross-disciplinary security reviews, peer code review and testing, vulnerability/penetration testing with static and dynamic techniques, independent reviews, etc. For this reason, an off-the-shelf application should not be modified by in-house personnel in ways other than those made available by the vendor as product configuration options.

Applications developed in-house have the advantage that they can be customized to meet the exact needs of the business. They also may be less expensive either initially, or over the life of the solution. However, they do pose several risks. One risk that is often overlooked is that such applications are often not reviewed or updated on a regular basis. Such an application may be secure when it was written, but new exploits are being developed everyday and an application that was once secure may no longer be so. Valuable and scarce resources, both human and monetary, are usually focused on the creation of new functionality and the delivery of new projects—not on the review and maintenance of applications that are still "running just fine." Those applications therefore fall further and further behind the technology curve and may become more and more vulnerable. Another risk is that security testing is likely to be less robust than for vendor-supplied solutions. Organizations that are not dedicated to the development of such solutions will likely not have the full scope of security testing resources available to a specialist. Such testing resources can be expensive and cost-prohibitive for businesses with a different core mission.

> *From the Standard*: Packaged applications should ideally not be modified. [12.5 Security in development and support processes] (ISO 2005).

From the Standard: Application system managers should be responsible for controlling access to [development] project and support environments. [12.5 Security in development and support processes] (ISO 2005).

From the Standard: Access to system files (both executable programs and source code) and test data should be controlled. [12.4 Security of system files] (ISO 2005).

Care must be taken when considering the cost of either approach. The decision to go one way or another often comes down to the cost of the solution. It is important that the total cost of ownership be well understood before this decision is made. Considerations such as the scope, ease of integration, need for professional services or support, platform or platforms on which the solution will need to run (Windows Server, Windows Desktop, Unix, Linux, Mac, etc.), the security, maintenance, reliability, expected life of the solution, etc. must all be included to get a real picture of the comparative costs. Sometimes, the solution with the lowest total cost of ownership is not what was expected.

Another element that must be considered, and one that is especially important for custom solution development whether in-house or externally, is the protection and integrity of the source code and the systems on which the solution is being developed, tested, and deployed.

Clear responsibility and accountability for the protection of the code and project systems must be given to the managers. Forty-eight percent (48%) of all data breaches in 2010 were from insider sources (Verizon and the U.S. Secret Service 2010) and it is imperative that action be taken to reduce the chances that a person with malicious intent can compromise the source code of the application or the systems on which the application is to run.

Review and Testing

One method that can help make it much more difficult for a malicious person to compromise a system during its development is to employ a rigorous program of review and testing. A certain degree of testing is always done, but this is usually focused on testing the solution for suitability for use, adherence to specifications, and smooth operation in the existing environment. What is usually done is "unit/functional/feature testing" followed by "integration/system testing." What is often ignored is testing specifically focused on the *security* of the solution.

Peer Security Review

Upon completion, all portions of a piece of written code should be subject to a security review by a *different* person. Again, peer review is often done to ensure that all the required functionality is included. However, this review should be specifically focused on security. Each line of code should be understood by that second person so that it can be confirmed that there are no backdoors, trapdoors, or other elements that could compromise the operation, integrity, or security of the application or the data that it will handle. It is important that this review be conducted by an experienced technical resource. Including such a review in the standard development process will reduce the chances that a single person acting alone can compromise the system by including malicious code.

Static Code Analysis

Once the peer review is complete and the issues resolved, the code should then be analyzed using an automated static code testing system. Such systems review the code looking for vulnerabilities and can sometimes even test for violations of best practice. Automated testing suites like these and the ones below are programmed with the latest lists of threats and vulnerabilities. Use of these techniques is a excellent step in showing due diligence.

Static Binary Code Analysis

Unless very strong code control is in place and rigorously enforced, it is possible that a malicious person could modify the source code after testing is complete, but before the code is compiled for production. Furthermore, modern coding techniques often rely on "includes"—items of precompiled code, functions or modules that are included in the compiled version of the code, but are not written into the actual source itself. It is possible that malicious code could be written into an include and therefore missed by a peer reviewer. Or more subtly, through the combination of the code in an include and elements of the new code, a malicious or insecure effect could exist that is not obvious from the review of either independently.

Static binary testing helps to mitigate these risks by conducting a code test on the actual compiled binary instead of the original source code itself. In its compiled version, the code now contains all the includes as well as the new source code written by the developer. This type of testing is therefore more complete.

Dynamic Code Analysis

There are vulnerabilities that cannot be tested by analysis of the static code. There are often functions that do not do anything until the code is actually running and interacting with other elements in the system. Therefore, code should also be tested for vulnerabilities when in place and running. If the development team is given a vulnerabilities scanner, they can test their own code in the development environment during the unit/functional testing and resolve any important findings before promoting that code to QA for system/integration testing. However, vulnerability testing should be done again in QA before the code is migrated to production. In the security field, separation of duties is often recommended as a way of preventing a single person from being able to compromise a system. Here again, the vulnerability test in QA and approval that the code may be released to production should be done by a group other than the group that did the first dynamic vulnerability test. If the development team did the Dev → QA test, a security group (or someone other than the development team) should do the QA → Production test.

Independent Testing

For applications of extreme sensitivity, or for code written and provided by an external group under contract, independent testing can be valuable. The additional level of testing and rigor achieved when engaging a group with the sole purpose of ensuring the security of the code/application/solution is a very strong statement about due diligence with respect to security.

This may also include special-purpose testing, if applicable. There are applications and information that are so sensitive that special testing should be included. Information classified as top secret by the government or the core competitive information upon which a company is built (the formula for Coca-Cola, for example) could be worth billions if compromised. The potential financial rewards make criminals eager to go after such targets. There are ways that information can be passed so as to be very difficult to detect. Steganography and covert channels, as well as Trojan code placed by a malicious insider, are examples of this. If you are dealing with this level of information, engage the services of a security specialist to assist in the development of a strategy and security plan.

Requirements for Testing

If a vendor-supplied solution is selected, the requirements document should address the types of testing and certification expected and a process for the remediation of findings. This rigor should also be applied to solutions developed in-house.

> *From the Standard*: Checks should be made for information leakage for example via covert channels and Trojans if these are a concern. [12.5 Security in development and support processes] (ISO 2005).

From the Standard: Purchased software should be formally tested for security, and any issues risk-assessed. [12.1 Security requirements of information systems] (ISO 2005).

Risk Assessment and Risk Acceptance Forms

One of the central tenants of information security is the belief that there are three elements that must be kept in balance: confidentiality, integrity, and availability. Most people think that information security is *all* about *confidentiality*—passwords, encryption, key cards, and the rest—making sure that only the right people get the information. People who have had more exposure to it understand that *integrity*—making sure that the right people get information that is correct and complete—is just as important. Only a very few understand that *availability*—ensuring that the information is properly backed up and that authorized people can get it when they need it—is just as important as the other two.

One implication of this is that there are times when it is the correct business decision to allow a system to go into production even if there are some vulnerabilities still present that have not been mitigated to the degree that would really be best. If the decision is between (1) delaying a critical update until a particular vulnerability is resolved when, in doing so, the business is denied a functionality required to compete, risking that customers may go to competitors and jeopardizing the economic viability of the business itself and (2) allowing the update to go forward with the security vulnerability still present, risking that the vulnerability will be discovered and exploited before proper mitigations or compensating controls can be put in place; the right decision may be to keep the business viable, keep people employed and move forward with the update, working as hard as possible to get proper mitigations and compensating controls in place as rapidly as possible.

However, it is critical that senior management be the people to make this kind of decision. They are the ones with the warring responsibilities of fiduciary duty and the duty of due care and due diligence.

It may even be something much less dramatic: Perhaps there is an older printer in the building that has an embedded FTP server that cannot be turned off. The organization does not currently have the funds to replace the printer, and so may choose to accept the risk that a hacker may exploit that FTP server to launch a denial-of-service attack from inside the company itself. This risk is moderate, not critical, and mitigation can be put in place by making sure that the printer's administrative password is set and is strong. Compensating controls are in place, but the risk still exists.

In these cases, management must be clearly informed of the situations, options, and implications of the available choices. It is then up to them to make the decision and set the direction.

A formal process of risk documentation and acceptance is helpful for this purpose. Formally writing up the risk in plain terms helps clarify what is really at stake and helps management with the decision. Recording the documentation helps drive clarity and transparency in the organization.

A Risk Acceptance Form (RAF) should include these elements as well as any others that may be helpful for the particular organization in question:

- Requestor name and department.
- Summary of the request.
- Overview of the service affected.
- Summary of how granting the request will put the organization at risk.
- Benefit of accepting the risk.
- Summary of controls in place to mitigate the risk (what is going to be done to lower the risk to acceptable levels).
- List of risk remaining after controls are put in place.
- Statement by the manager of the requesting department that they feel that the residual risk is acceptable and why.
- Signature block for business owner and for the technical owner. One of these two is likely to be the person requesting the approval. This request should be made with the concurrence of the other.
- Decision signature block for the organization's director of information security or other designated risk manager. Typically, this person will evaluate and approve or suggest changes that should be made before approval being granted.
- Decision signature block for a senior manager with the authority to make risk decisions for that organization—such as the CIO. This is usually only required if the risk manager does not feel the risk is acceptable but the business insists that no other approach is feasible. The risk is to be evaluated and final decision made by that person.

One important point to consider: Documents such as this provide very sensitive details and would be a great find for a competitor or malicious person. All documents that include these kinds of details must be treated as confidential and protected, both during their creation and after their approval.

At first, a formal process of risk acceptance such as this can make people uncomfortable. They often feel that the form is a way of pointing a finger at them in case something goes wrong. In fact, the *opposite* is true. If a developer, knowing there is a vulnerability in the application, puts that application into production without telling anyone about the vulnerability and without mitigations, it is *then* that the

> *From the Standard*: Access to system files (both executable programs and source code) and test data should be controlled. [12.4 Security of system files] (ISO 2005)

developer is at the most risk. That developer just made a risk decision on behalf of his or her company without the proper authority to do so. If the worst were to happen, it is that developer who would bear the responsibility and the consequences. If, on the other hand, that developer documented the risk—showed that the mitigations that could be done would not cover all risk, and that there are still a few issues—and sent that document up for approval, that developer is better protected. He or she let the situation be known and let management decide if the potential benefit was worth that risk. Management is the group charged with the authority to make that judgment call.

Implementing

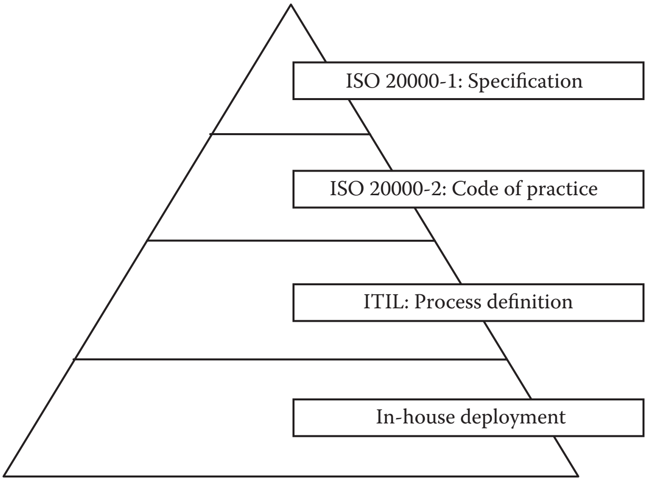
Implementation of the completed and tested solution is full of challenges. Plans must be made and executed for the coordination of required implementation resources, training of users and support staff, support processes, and many other elements. Before implementation, the operating environment should have been set up according to the plan, but postimplementation is the time to confirm that it was indeed set up as intended. Verify via audit that the solution as it actually is in production includes the controls and protections that were included in the design.

Maintenance and Control

Once the system is implemented and goes into normal operation, it must still be controlled.

ISO 20000 and IT Infrastructure Library

ISO 20000 and IT Infrastructure Library (ITIL) provide the best practices for IT management. ISO 20000 (http://www.iso.org/iso/catalogue_detail?csnumber=41332) is an international standard for IT Service Management. It provides, as do so many other ISO standards, information on *what* needs to be done. The ITIL (http://www.itil-officialsite.com/) is the most complete set of best practices on *how* to do it (ISO 20000 Central 2005). Although ISO 20000 and ITIL are not actually security standards, an organization run by them *will* have better information security than an organization that does not, all else being equal.



ITIL version 3 is made up of five volumes: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. The elements of ITIL that provide the most benefit to security are

- Risk Management (in the Service Design volume)—Engages the community in understanding and qualifying risk and helping to mitigate it
- Availability Management (in Service Design)—Supports business continuity
- Service Continuity Management (Service Design)—Supports business continuity
- Information Security Management (Service Design)
- Service Asset and Configuration Management (Service Transition)—What you have and where it is located
- Service Validation and Testing (Service Transition)—Confirms that the system is properly tested before implementation
- Change Management (Service Transition)—No change is put into place without proper testing, validation, and approval, which improves service stability and reduces the possibility that a malicious person can sneak something into production
- Incident Management (Service Operation)—Security incident response will often require that IT personnel be engaged
- Problem Management (Service Operation)—Patterns of incidents are collected into problems and solutions are developed, increasing the stability and security of the system
- Access Management (Service Operation)—Access control is a key concern of information security

From the Standard: Formal change control processes should be applied, including technical reviews. [12.5 Security in development and support processes] (ISO 2005).

Audit

Larger organizations are typically subject to audit requirements and many also have an internal audit group. From a security perspective, audits can be great opportunities to highlight and get support for security issues that may be present in an organization. Internal audit and information security often have very similar goals and can work together to help the organization achieve stronger controls.

Managing Information Security Concerns in a Maturing System

As the system matures, there will be ongoing information security concerns. Incidents will need to be managed, problems resolved, changes properly reviewed, tested, and controlled, etc. Many of these activities are simply the reapplication of techniques and process described above, but there is one thing that is often overlooked when a system has been running stably: That system should continue to be reviewed and tested for vulnerabilities on a periodic basis.

An application that was developed in-house, according to the best practices of software coding and information security and IT service management, may still pose a risk as it ages. New vulnerabilities are discovered everyday and new exploits are being written for those vulnerabilities. A piece of software, even if it was once secure, may become less and less secure with time. The organization should monitor security organizations for information relating to new vulnerabilities and alert management if something is released that could pose a threat. Development resources must be given time to focus on responding to those emerging threats.

> The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus, his person is not endangered, and his States and all their clans are preserved.
>
> **—Confucius**
> *Chinese philosopher and reformer (551 BC–479 BC)*

From the Standard: Technical vulnerabilities in systems and applications should be controlled by monitoring for the announcement of relevant security vulnerabilities, and risk assessing and applying relevant security patches promptly. [12.6 Technical vulnerability management] (ISO 2005).

Legacy/Retiring/Closeout/End of Life

Systems become obsolete, the programming language that an application is written in depreciates, the type of hardware that the solution runs on is no longer supported, the business wants to move to a different solution, a strategic decision is made that services will be outsourced or in-sourced or right-sourced; whatever the reason, there will be times when an existing system falls out of support or comes to the end of its useful life. When this occurs, it is important to consider security.

Businesses often make the decision to continue using a system or solution that is no longer supported by the supplier of the hardware or software. There are often good reasons for this, but there are also risks. The longer a system is in place, the longer there is for vulnerabilities to be discovered. If the system is no longer under support, there are no security patches forthcoming from the vendor. If the business opts to continue using such systems, they assume responsibility for detecting and developing solutions to emerging security threats.

If the system is to be closed out or replaced, there are other considerations. What is going to happen with the data housed on those systems? How is it to be retained and protected? What will happen to the physical hardware?

Data, once written to the hard drive, stays on that hard drive until overwritten. Deleting the file does nothing but remove the file's name from the computer's list of files. The file itself is still there and can be recovered easily. That is, it can be recovered until the file is overwritten or destroyed in some other fashion, such as by "wiping" or "shredding" it. If the hard drives from an old computer are discarded or released to another organization before being properly sanitized, whatever is still on them may be recovered by whoever happens to get their hands on them. It is not unheard of for old computer hard drives to be sold on eBay, only to be bought by someone who went through them with software that can recover deleted files and who found files containing credit card numbers, social security numbers, banking information, architectural blueprints, and construction details for major public buildings, etc.

As an aside, this risk also applies to photocopiers and office printers. Many of these devices contain a hard drive onto which print jobs are written (or spooled) while waiting to be printed. This means that when a printer or copier is thrown away or given back to the vendor, weeks, months, or years of print jobs may be present on that hard drive. Who knows what sensitive company information may be present?

Conclusion

Throughout the life of an information system—defining the business goals, specifying the details of what is needed to achieve those goals, purchasing or building a new system, testing it, training people on it, putting it into production, using it and maintaining it throughout its lifetime, and then, eventually retiring it and moving to something else—there are many information security issues that must be considered. These considerations must be made an integral part of the planning and decision-making process.

This chapter provides some information on the types of considerations that will be encountered, questions that should be asked, and decisions that will need to be made. If it is an organizational goal to improve systems security and compliance, personnel experienced with security and its application to the field of information systems development, acquisition, and maintenance should be engaged and integrated with the project team responsible for these activities.

References

Beck, K., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R.C., Mellor, S., Schwaber, K., Sutherland, J., Thomas, D., and Beedle, M. Agile Manifesto. February 2001. http://agilemanifesto.org/ (accessed August 24, 2010).

ISO 20000 Central. *ISO 20000 Central.* 2005. http://20000.fwtk.org/20000-itil.htm (accessed August 30, 2010).

ISO. ISO27002:2005 (June 2005): 77–89.

Ives, B., and Learmonth, G.P. The information system as a competitive weapon. *Communications of the ACM* 27, no. 12 (December 1984): 1193–1201.

Krutz, R.L., and Vines, R.D. *The CISSP Prep Guide: Gold Edition*. Chap. 7, 337–362. Indianapolis, IN: Wiley Publishing, Inc. (2003).

Lillard, R. Getting wise to the counterfeit market: System life cycle design threats from counterfeits. *Wireless Design and Development* (July 1, 2009): 8.

Mulcahy, R. *PMP Exam Prep.* 4th. RMC Publications (2002).

Peslak, A.R., Subramanian, G.H., and Clayton, G.E. The phases of ERP software implementation and maintenance: a model for predicting preferred ERP use. *Journal of Computer Information Systems* 48, no. 2 (2008): 25–33.

Ponemon Institute. *2009 Annual Study: Cost of a Data Breach.* Ponemon Institute (2009).

Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK Guide).* 2000. Newtown Square, PA: Project Management Institute (2000).

Sherstobitoff, R., and Bustamante, P. You installed Internet security on your network: Is your company safe? *Information Systems Security* 16, no. 4 (July 2007): 188.

Slade, R.M. Application security. Chap. 8 in *Official (ISC)2 Guide to the CISSP CBK*, by Harold F. Tipton and Kevin Henry, 537–629. New York, New York: Auerbach Publications (2007).

Trompeter, P. *A Comparison of Software Development Lifecycle (SDLC) Models.* Paul Trompeter LLC (August 2008).

Verizon and the U.S. Secret Service. *2010 Data Breach Investigations Report.* Verizon (2010).

Chapter 11

Information Security Incident Management

Brad Smith

Contents

Overview

As the Information Age matures, the data residing in various locations becomes more valuable. More value usually always equals more attempts to steal that data. This section will help you understand the concepts of information security incident

Term	Usage
Event	Observable occurrence in a system or network
Adverse event	Negative consequence event, i.e., system crash
Computer security event	Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, i.e., DoS, worm

Figure 11.1 Definitions.

management. Remember the old phrases, "It's not if, it's when" and "Forewarned is forearmed," and you'll have the essence of this chapter.

Incident response (IR) and management is similar to working any disaster. Certain concepts have been developed and can be utilized, whether it's a computer security event or a natural disaster. These basic concepts have been categorized into several helpful documents such as the National Institute of Standards and Technology's (NIST) 800-61 "Computer Security Incident Handling Guide," the Department of Homeland Security's (DHS) "Privacy Incident Handling Guide," and the United States–Computer Emergency Readiness Team's (US-CERT) numerous publications.

So we're all talking apples to apples, in this chapter we will be using the definitions provided in Figure 11.1.

Why Do I Need Incident Handling?

Although most people would say it relates to the law—and for good reason—here is what some federal laws say about IR.

Federation Information Security Management Act of 2002

> "…Each federal civilian agency must designate a primary and secondary point of contact (POC) with US-CERT, report all incidents, and internally document corrective actions and their impact. Each agency is responsible for determining specific ways in which these requirements are to be fulfilled."

Office of Management and Budget Circular A-130

> "…Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats."

Federal Information Processing Standards

> "…Minimum security requirement for federal information and information systems requires incident response."
>
> NIST 800-53 "Recommended Security Controls for Federal Information Systems"

So if you work for the federal government, you need IR because it is required by law!

If you ask any good businessperson, they'll understand that it's to keep the business in business. Many companies are now in the class of "technology dependent," which means that without their technology, they're not in business. Think of all the businesses you know; how many of them could continue to function without their technology?

Having a systematic method to quickly recover from an incident and continue with business as usual is the reason it's driven in the private sector.

Another great reason for incident management is the learning process needed to fix future problems. How long has the SQL injection hack been successful? Do people really fix the problems or do they just apply a light gauze dressing and think they'll fix this in the future?

Response by Size

Think about IR for these two different businesses.

MegaMed is a large medical chain distributed across 12 states. Hundreds of small clinics and doctors' offices are under the control of the MegaMed IT Department. The Network Operation Command center has just detected a worm brought in by someone downloading the "Whack-A-Mole" game onto a remote PC. Their real-time network intrusion prevention system and continuous threat-monitoring system notified the center and quarantined the system. The remote malware cleaner has already started removing the mess and, within minutes of the incident's start, the incident is over. Response reports are documented and the incident case is closed.

NanoMed, run by Doc Bob and Doc Bill, is a small medical office. Bob's wife does the books and Bill's wife, who is a registered nurse, helps with the patients. Bob's wife really likes the new Whack-A-Mole game she downloaded from the Internet. Everybody agrees that the computer is running slower but, well, that's just the way they get. Bob and Bill are having dinner together when they start to discuss the problem of several customers having reported their identities being stolen and worry if they'll receive payments from these customers.

What can we learn from these two businesses that suffered the same event? The same threat materialized into a computer security event and the same laws cover both entities relating to IR. But, are they the same response?

When you're designing an IR program, consideration must be given to the resources, knowledge base, and true understanding of what the customer will really do versus what they should do. Would an up-to-date anti virus catch the Mole problem? Numerous times I've seen plans for incident management pushed out from on high and totally fail when used in the receiving entity.

Please don't think that bigger is always better. Look at all the large businesses that have been breached even though they had gobs of money to spend. Just consider the reality of the business when conceiving your incident management plan.

Policies and Procedures to Smooth the Incident

IR probably gets the least respect and money—until something happens. Good programs understand how to create paperwork that will give them the power to make the program successful. Starting with a top-down approach, let's see what policies and procedures you could use:

- Start with a statement from upper management announcing that IR is an important part of a plan to keep the business running, even if a major security event occurs
- Remind people what IR is by adding small articles to the newsletter. These are designed to keep IR on a top-of-the-mind position
- Update the IR policy and procedures regularly. It would be best to build these reviews into the policy itself so that they must be kept up-to-date
- Update when new management comes in. These transition times are a great opportunity to expand awareness by management of the needs of IR

Here are a few policies and procedures that help in establishing and running an IR easier:

Overall security IR policy with definition of terms related to an incident. This policy should delineate the roles, responsibilities, and level of authority of the IR team. Reporting mechanisms to meet legal requirements as well as a severity rating (prioritization) of incidents need to be included. Forms, reports, contacts, and an organization call tree by title need to be included.

Policies and procedures that delineate performance-monitoring standards and a system to track the statistics of incidents over time and remediation of the security events need to be established so the organization has a longitudinal view of the incidents they have encountered.

Specific procedures are also needed and these *should* flow from the policies. Standard operating procedures for response should include technical processes to use, checklists, and forms to be used in the response. These procedures should be as detailed as possible—listing software and how-to's for each event that might occur. Utilizing these procedures will help reduce stress on the team, reduce training, and provide continuity across the entire organization. Procedures should always be mappable to the policy so they can be considered as one unit with two parts.

Again, consideration for the size of the organization must be given in developing a team. Multinational organizations suffer from regional misunderstanding (Red is good, yes?), whereas small organizations have few qualified people, few policies/procedures, less capital for incident management, and an increased risk of their plan failing.

Although these policies and procedures seem like a simple list to obtain, just keep that thought while they're being pushed through the chain of command.

Models of Team Structures

The current literature reviews show that there are three types of team structure in use.

Central IR Team

This is used by large organizations that are only minimally geographically distributed. The team is located at a central location and dispatched to needed locations. Pros for a central team include a central staff with up-to-date skills, standardized response to incidents, and set a unified policies and procedures for the organization. Weirdly, this is also what's happening in small businesses, where Dr. Bob's brother comes over and says "Yep, you're infected" and cleans it off.

The cons for this design include the dispatch time for the team, travel costs, and if the team is not supported properly or trained properly, the entire business gets bad service.

Distributed IR Team

This method has teams, located in several geographically disperse areas, which respond based on location or business division. A central incident control is still needed to coordinate and provide a unified methodology for all the teams. Training requirements, recruitment, and increased need for highly trained professionals are all cons for this system, whereas rapid response and specialized teams based on security clearance are easier to construct. Usually used by large international organizations or national governments.

Coordinating Team

This team structure is designed to help less experienced teams, particularly in a complex situation or in a wide-scale cyber disaster. The coordinating team often advises other teams but has no true authority during the response. When US-CERT or the FBI takes control as the overriding agency or when a manufacturer dispatches a team to help a customer is an example of this type of team. These teams are packed with experts and are wonderful to have watching your back. Cons are if you get one of these, you probably already have a bigger mess than you think.

Most teams today are simple central IR teams but consideration of all types of teams should be based on the type or genera of the business.

Team Staffing Models

Current staffing models are based on how often you utilize the team.

Employee Staffed

These are your employees who are specially trained to manage incidents. Utilizing a 24-7 model of response, these teams can be equated to the fire department, which waits for an event and responds appropriately. Many employee teams are assigned additional duties when they are not in use. These teams can be highly stressful and can suffer from high turnover rate.

Partially Outsourced

This team is constructed of full-time and part-time staff utilized from a third-party source. Both the organization's staff and the outsourced staff work together to solve the event. Conviviality requirements of the outsourced should be addressed and well as total cost of services. (Who pays for food, tools, and lots of other tiny expenses that show up during an IR?) The organization's help desk, based on policy, usually makes the decision to activate the outsourced team if an event happens.

Fully Outsourced

These are companies that specialize in security services. They often offer monitoring 24-7 firewall, intrusion prevention system (IPS), and intrusion detection system (IDS) services. When an event is noted, they dispatch the team. Many managed security service providers use this staffing model. The contracting organization is notified of an event when the fully outsourced team is dispatched.

The staffing model picked needs based on the frequency of events and the human resources available. Costs do vary but the total cost of the event should be considered when picking the staffing model.

References from previous customers for any outsourced team should be sought; turnover rate of the team, written responsibilities, and training records should also be reviewed before selecting a team. Lastly, the decision on who can disconnect computers from the network/Internet needs to be defined. Loss of revenue when disconnected could be great, so having the decision on who can shut down the business process is needed before an event occurs, not during.

What's the Team Really Cost?

Hidden costs abound when deciding on staff and team design. Here are a few items to consider: training costs, travel/per diem costs, physical security for the team, and employee churn rate all are hidden costs when deciding on team design. Proper consideration to design is needed to keep the team from failing before it's even started.

Team Personnel

IRs are stressful times, not everybody can be successful on an IR team so good interview techniques and even stress interviews should be used when selecting staff. Each job on the team is different and needs a different type of person for each task. These are the standard jobs on an IR team.

Team Manager

This is the team boss. They are technically adept, have excellent communication skills, and work well under pressure and can guide others who are also under pressure. Team managers are usually seasoned veterans of IR and set the tone for the team. Do they keep their skills up? Are they cool and polite during the event? The "personality" of the team is usually a reflection of the team manager. Select this person carefully.

Deputy Team Manager

This is the backup for the team manager. This is the person who will evolve into a team manager. The same considerations in the selection of the team manager should be given to selecting this person.

Technical Lead

This is the techie of the team. They don't need people skills because their main job is the technical responsibility for the event. A high level of IR skills, a drive to continue learning, and a gnawing desire to get the truth from the event is needed. This job really controls the quality of the team's response.

Incident Lead

Think of this person as the logistical support for the team. They coordinate with other teams and special handlers, provide updates to other groups, ensure the team has what it needs, and handles the food, lodging, travel, and "duties as needed" for the team. Skill in people-handling and logistics are more important than wicked good techie skills. A good Incident Lead can keep the stress off the team by letting each person do their own job without worry of where they'll stay or if they are going to get something to eat. The best Incident Lead would be Radar from the old *MASH* TV series; he knows what you need before you know you need it. Select this team member with the same care as Team Manager because they can quickly lower the quality of work done by the team. Ever worked when you were hungry and tired? You'll understand why this is one of the most valuable members of the team.

Team Member Variables

Many different books/organizations have different jobs included in this list. Please do not take this as the only way of staffing teams. The US-CERT includes an Incident Coordinator whose job is to be the overall coordinator of the team and a First Responder who does what the name says.

Helping the Team

IR is a stressful job providing little room for error. Team members are equivalent to racehorses that need special handling to perform at their max. Planning for the growth of the team (Do you think the number of incidents are going down anytime soon?), allowing them to work on pet projects when not on team duty, rotation of members on/off team so you have a full cadre of help, giving members uninterrupted time off, and a hot meal at least every 12 hours can all work to decrease stress and team churn. Establishing a mentoring program or an exchange program with other teams heightens skills, as does the development of response scenarios, and advanced training also reduces stress and grows the team. Most of these techniques have little or no additional cost to the organization. Many organizations utilize the IR team by performing internal penetration tests or improving their skills on new tools/techniques.

Who Needs to Be Involved?

Many people get involved in a team when it's being established. Here are just a few and what is needed from them.

Senior Management

They need to endorse and support the entire program. Management needs to be informed of each event and how the team performed during that event. As always, senior management has the responsibility to the shareholders to protect the data and minimize the effects of a computer security event.

Information Security Area

A clear definition between the information security and IR teams needs to be established. The Incident Lead is usually involved with this department to help smooth any conflicts that may arise.

Telecommunications

Proper communications between the team members and management involves the telecommunication section. Special phones or voice over Internet protocol (VoIP) connections for team–team private communication is needed to maintain the confidence of data as well as communications with outside organizations are considerations when establishing the communication needs of the team.

IT Support

Laptops and tools used by the IR team are specialized and need to be more powerful than a standard corporate world PC. Many teams use "gamer" machines because of the additional processing and storage power they offer. The use of virtual machines to work with attacks is increasing and thus a large storage capacity is needed. Advanced antimalware (AM) as well as an IPS system to minimize cross-infection between compromised machines and IR team machines is of prime importance. Proper cleaning of IR team laptops postincident is also a large postevent task.

Legal Department

Allowing team members to have their questions answered in a timely manner by the legal department is important to keep the team from stressing about going to jail. That decision to unplug the compromised machine has heavy repercussions on revenues and should have the legal department's view if there is any question. Teams without adequate legal support turn timid in their response and delay making important decisions.

Human Resources

Hiring, disciplining, and dismissing team members are the realm of human resources (HR). Helping HR understand the skill levels and type of person who will work well on the team is important. HR is also the keeper of policies and procedures so having their help in revisions and updates is vital. Most HR professionals are willing to listen and help select the proper staff. Low team turnover makes their job easier.

Media Relations/Public Affairs

The technical level required by a team leaves only the Incident Lead to handle outside requests for data. The ability to utilize additional media services to help in the control of the event is critical. Unconfirmed rumors can do more damage to a business than the actual event does. Early press releases reassuring customers that everything is OK is important as is a constant update of the situation. Even the old "ongoing investigation" comment helps reduce stress during the event.

Physical Security

Most people who have never done IR can't see why physical security is needed. Keeping employees or press out of the team's way is vital. Crowd control and protecting the physical evidence are great jobs for physical security. Several incidents of reporters sneaking in to watch the team have been found. Physical security is a good way of maintaining the confidentiality of the incident and the data involved. During many events, the guards feel useless and they truly want to help. Assigning them to the team for protection helps them, and the team, feel that they are in control of the situation and part of the team.

Business Continuity Plan

Your business continuity plan should be active during an event. This is the chance to see if your plan works and the time to see what modifications should be made. The team should have a copy of the plan available to them so that they can verify that the path they are treading is correct.

Summary of Team Construction

There are many little parts needed to establish and run an IR team. A properly run team will yield a proper response to almost any security event. IR team members have to face stress during the event because they realize that the fate of the business is in their hands. How fast can the event be resolved? What data was compromised?

What can be done that will keep this from happening again? Did they really get all the backdoors? Think of the team as a SWAT team that can save your business when done properly or kill the business if done improperly.

Steps to Establishing an IR Team

There are nine steps outlined by the NIST in establishing an IR program and team.

1. Establish IR capacity: Decide how many people are needed for a 24-7 team. Calculating a full-time team means having 1.5 to 1.7 people per job per day. People get sick, take vacation, have personal problems, and like to sleep, so we need more people than just an 8 to 5 shift.
2. Create an IR policy: What is an incident? It seems simple but what it is, how to respond, and who responds are basic issues that need to be decided upon when designing the IR policy. Decisions of where the team sits in the organizational structure and specific roles/responsibilities are established in this document.
3. IR based on IR policy: This is the roadmap of implementation. What are the short-term/long-term goals of the team? What metrics are needed to measure the team and its member's effectiveness? What will be the staff's training requirements and the staff's hire requirements.
4. IR procedures: These are the detailed procedures that establish how to work with different events. These are based on the IR policy and the needs of the organization. Procedures are the tasks needed to actually correct the event.
5. IR communication plan: This plan involves dealing with third parties who are involved with the event. Public affairs, legal, and C-levels are included in this plan because it is the "face" the organization will give to the public. Experience shows that it is better to use a trained person rather than the CEO to deliver bad news because most CEOs have little knowledge of technology and can actually make the situation worse.
6. Select the team model: Is the team full time in-house? Fully outsourced? Ask other organizations similar to yours what model they are using and what is good/bad about the model. Review the advantages and disadvantages of each model to help decide which one is best for your organization.
7. Select the personnel: As discussed previously, there are multiple models of how team personnel should be selected. Finding technically skilled people is critical to the team and finding people who can handle stress will keep the team functional. Team-building exercises can help a new team feel confident in each other and in the leaders of the team.

8. Determine services: Decide on what the team should be when not in response mode. Several large corporate teams are used as fully outsourced teams to other organizations, whereas some just stay within their own organization. The size of an organization does play a role in determining the number of services offered.
9. Notify other groups: Public notification of other response teams is important. This allows opportunities for cross-training or technique sharing with other IR teams in the area. Press releases about team services can help the entire organization understand the roles and responsibilities of the new team. Also, a "coming out" party can help all the team, management, legal, and staff feel comfortable in their roles involving the team.

Most organizations find that getting the team established is the easy part, keeping it from falling apart is the hard part. Support from management wanes as time goes on, staff members change, leaders change, and organizations' need for the IR team changes over time as the business changes.

Doing the Response

Response can be broken down into several steps. Here is the typical flow of a response: preparation for IR → detection → analysis → containment → eradication → recovery → postincident activity → repeat to preparation.

Let us now review each step and the tools/resources needed for each step.

Preparation: Organizations that have an IR team can utilize the team for inside testing. By performing regular penetration tests and risk assessment on the organization, a "prevention is the best policy" thought process can be started. Find the errors before you need the team to fix them.

Detection: Knowing the signs of an impending or current event is crucial. Often, the organization doesn't know they have a problem until formal audit finds evidence in a log review. Here are a few ways of determining if you have a problem:

- IDS, IPS, firewall logs
- Host, OS, app logs
- AM alerts
- File changes found with file integrity checker
- New vulnerability report from a reliable source
- Software listed on sites like www.Exploits-DB.com or www.Insecure.org that is not patched
- Multiple disgruntled employees
- Warning from other teams/organizations about current events
- Egress reports of data to strange addresses

- Large amounts of data leaving your business for some unknown location
- Your network is just running weird

Incident Analysis: What is the normal traffic profile of the network? Where are the central logs and is there a correlation of log events? Are all the clocks synchronized or do you have to look for time offsets to determine the true time correlation? Run packet sniffers and verify results. What does the knowledge base say about the data? Are you utilizing an event diagnostic matrix? What does the team's gut say? Experience is a huge benefit during this stage.

Incident Containment: How can you contain the event the fastest with the least residual damage? Often, people think it's as simple as unplugging the machine in question and running some cleaner program (if only). How can you track which other machines or what data is missing when you can't see the flow out of the infected machine? Moving the machine to a separate switch with honey pots and sniffers can show you what and where your data is going and how it's infecting other machines on your network. The need to preserve evidence is important in this step. No prosecution can occur with valid evidence handled in a proper chain of custody methodology. On a good day, it is as simple as unplugging the machine and running a cleaner. In the IR business, good days are getting fewer and responses are taking more days.

Eradication: This is one of the simplest steps. Just reload the machine from a standardized ISO image and off you go. Monitor egress from the network to make sure no other machines are still infected. Then, it's off for coffee. When a widespread worm hits, pulling all the machines off the network and rebuilding them can take several weeks or months, depending of the size of the event.

Recovery: Several manufacturers have a protocol for reestablishing the needed services on the network. This should be done in an orderly manner with special attention given to the line of business software. The speed and accuracy of the recovery can determine if the business survives or not.

Postincident Activity: Now is the time for education of the employees and IT staff. The freshness of the event helps people understand that employees can cause security events. Documentation, which is ongoing during the event, is correlated and formalized into an event document. Team evaluation of performance and the metrics of success as well as debriefing the team are done in this section. After a particularly difficult or long event, the team may need some additional help in relieving the built-up stress. This is important in an unsuccessful event when substantial loss has occurred. Important data related to the event includes

- Lessons learned
  - What happened?
  - What could be done sooner?
  - What steps could be improved?
  - What tools did we need?
  - How well did we do?

- Assess data collection
  - What else did we need to know?
  - How can we use this in the future?
  - What was the precursor of the event?
- Analysis
  - Number of incidents handled
  - Time per incident
  - Total time of incident
  - Elapsed time to response
  - Team response time
  - Did logs and forms comply with established policies and procedures?
  - Subjective feeling of team

Repeat to Preparation: What happens to one business will happen to several of the same genera. Are all the other areas covered against this threat? What precursors were noted before the event and how can a monitor be set to alert if this event starts again? Review your policy and procedures to see what could be improved or which steps could be eliminated to speed the process up.

Incident Documentation

The Incident Lead is responsible for documentation being complete and accurate. A major problem is when each member documents the time based on their own timepiece. Make sure a coordinated time source should be selected and used by all team members. The largest amount of work is recreating an event document in which five different time sources were used. When did what really occur? Could it stand up in court?

Team Communication

The team members should be kept up-to-date on the current status via a secure communication method. Something as simple as hourly team updates in person should work as would cell phone updates to critical members of the team. Summary of incident findings, actions taken thus far, and evidence gathered should also be communicated to team members. Comments/feelings/impressions of team members as related to the event should also be discussed by members and team leaders.

Team Forensics

Many people can perform forensic analysis on a computer but not all of them can do it correctly or stand up to a prosecution attorney. Don't let anyone do the

Tools of the team
Tool/resource
Baselines of network: how has the network changed?
Blank media: for validation
Contact information: team, law, legal, e-mail, public keys, team off-hours phones
Encryption software: team communication, required by Federal Information Processing Standards
Evidence accessories: cameras, audio recorders, chain of custody forms, evidence bags/tags, pens, tape, gloves
Favorite software: forensics, packet sniffer, protocol analyzer, etc.
Forensics workstation: backup devices, machines for ISO, Helix
Hashes of files: used to speed analysis, verification, and eradication
Incident report: report method for both customers and staff
Laptops: portability
Network diagrams and lists of critical assets: know what you're working with
Network documentation, port lists: reference
On-call information: escalation method, number
OS, security patches, backup images: if available
Portable printer: log printing, on-site work
Secure storage: old reports, logs
Spare hosts: test virus, now virtualized
War room: where the action is taking place! once in command, don't leave!

Figure 11.2 IR tools.

forensic analysis if they are not trained and certified because you can disqualify good evidence that might win the case. Is this case going to court? Start thinking E-discovery requirements (Figure 11.2).

How Critical Is It?

There are several methods of determining how critical the event is. The higher the critical score, the longer it usually takes and the more people usually get involved.

Two different scoring mechanisms are in use. These are based on the different standards used by the NIST and DHS.

NIST Method

Let's start by reviewing the NIST standard. Here is the formula used in the calculation:

Severity = (current effect rating * 2.5) + (projected effect rating * 2.5) + (system criticality rating * 5)

Simply start by evaluating the effect the event is currently having on the business and what that effect will have in the future. So, it's how bad it is now and how bad it can get. Figure 11.3 is the chart to see what value to use for the effects the event is currently having and what the effect will be in the future.

Now we add how many systems the event affects. The definitions are given in Figure 11.4.

Value	Rating	Definition
0.00	None	No effect
0.10	Minimal	Negligible effect on one business/agency
0.25	Low	Moderate effect on one business/agency
0.50	Medium	Severe effect on one business or negligible on multiple agencies
0.75	High	Moderate effect on multiple agencies or infrastructure
01.00	Critical	Severe effect on critical infrastructure or multiple agencies

Figure 11.3 Effect rating definitions.

Value	Rating	Definition
0.10	Minimal	Noncritical systems (workstations)
0.25	Low	System supporting a single agency (DNS…) but single agency only
0.50	Medium	Mission-critical systems for single agency
0.75	High	Systems that support multiple agencies, critical infrastructure (root DNS…)
01.00	Critical	Mission-critical systems for multiple agencies or critical infrastructure

Figure 11.4 Criticality rating definitions.

Value	Rating
0.00–00.99	None
01.00–02.49	Minimal
02.50–03.74	Low
03.75–04.99	Medium
05.00–07.49	High
07.50–10.00	Critical

Figure 11.5 Incident impact rating.

Using the formula above and plugging in the values from the accompanying charts, you can now calculate the severity of the incident. Utilizing this number can give you an idea of how good/bad the incident is and how many resources need to be allocated to the event (Figure 11.5).

It is important to note that not all events are the same (doh!), so you can decide which events are major events and which happen all the time.

ITIL Method

ITIL breaks incident management down to

- Classification and initial support
- Incident detection and recording
- Investigation and diagnosis
- Incident closure
- Resolution and recovery
- Ownership, monitoring, tracking, and communication

DHS Method

The DHS takes a completely different approach to incident management. The system is broken into short definitions with short responses. This is more concerned with the overall protection of the United States than the virus on a corporate computer. The three stages are

- Low—which includes viruses and worms, the normal stuff
- Medium—these are targeted attacks on business or a particularly virulent Trojan
- High—acts of cyber terrorism, loss of public service, loss of computer-aided dispatch

Class	Problem	Time frame
0	Network testing	NA
1	Unauthorized access	Detection in 1 hour
2	DoS	2 hours
3	Malicious code	Daily (1 hour note)
4	Improper usage	Weekly
5	Probes, attempts	Monthly, classified 1 hour
6	Investigation	NA

Figure 11.6 Incident management and time frame.

This simple method is being taught to civilians around the country with the Sentinel Project. Although it may not be the best for business, it works perfectly well for rating events on a national scale.

US-CERT Method

The US-CERT also has a method that has worked well based on incident management and time frame. The chart in Figure 11.6 easily explains their system.

They also have a method of defining event criticality. These are the three basic types of events according to US-CERT:

- Normal—everyday events that don't require upper management's involvement
- Escalation—an event that affects critical production systems requires a change in the control process of the critical systems escalated events require senior personnel and notification of stakeholder
- Emergency—an emergency is an event that might affect the health/safety of people breach critical controls systems affect systems or stop activities, which affects the health/safety of people deemed an emergency as a matter of policy or by declaration of the available incident coordinator

CERT has a great program to help you understand their method. Please take advantage of this resource to give another system of evaluation to the computer security event.

Tools of the Trade

Having the correct tools makes any job easier. It's bad form to keep having to buy/borrow/steal things you need to complete the mission. While you are developing a jump kit that fits the needs of the organization, these are some of the basics. We

Initial incident-handling checklist	Done
Determine an incident has happened	
Analyze precursors and indications	
Look for correlation information	
Perform research	
Handler calls incident—begin documenting, investigation, and evidence gathering	
Classify the incident according to category (DDoS, code…)	
Follow incident category checklist	

Figure 11.7 Incident-handling checklist.

Generic incident-handling checklist	Done
Detection and analysis	
Prioritize incident based on business impact	
Identify resources affected and forecast which will be affected next	
Estimate current and potential technical effects	
Report incident to appropriate internal/external personnel	
Containment, eradication, and recovery	
Acquire, preserve, secure, and document evidence	
Contain incident	
Eradicate incident	
Identify and mitigate vulnerabilities exploited	
Remove malicious code or other problems	
Recover from incident	
Recover affected system to normal state	
Confirm systems function normally	
Postincident activity	
Create reports	
Hold lessons learned session	

Figure 11.8 Generic incident-handling checklist.

keep these items in old cyberevent bags so that when we need to go, it's all packed in one place. It's important to also keep track of *your tools* because nefarious people might want to disrupt you from completing your task. Figures 11.7 and 11.8 are checklists to give you a quick initial incident-handling guide.

Summary of Event Severity

Determining the severity of an event can help you quickly determine if extra help or a prolonged event is about to happen. The standard method used by the NIST is a favorite because it determines current and future effects on the business. The team that is properly equipped and has some idea of the problem they are about to encounter is much more likely to succeed than a poorly equipped and improperly informed team.

Responding to Incidents

The severity score really comes into play when you start deciding how to respond. We tend to break responses down into a simple system of short and standard terms. Usually, the higher the severity score, the longer it will take. How long does the incident management for the loss of a laptop go on? Weeks? Months? This is the "standard" length of most incidents.

Think about how quickly we now catch most malware and how easily it's removed. This would be a short term. Remember that the same steps of managing any incident uses the same orderly steps we talked about earlier, it's just that they are done quicker and easier. Let's look at some short-term incident management responses to common cyber events.

Viruses

This is where due care really pays off. A central management console to monitor the AM software is available from almost every vendor. Here are a few things you might do: Discontinue use of the infected computer, mark with physical sign if needed to ward off users, use a commercial malware cleaner, and verify that no other computers/media were affected, especially USBs and monitors for unusual activity.

Worms

Worms can wiggle their way through the network before most companies know it's there. Quality AM scanners and use of packet sniffers internally will all help in making these decisions. Ask the user if they have had strange messages/behavior on the computer. Check firewall for strange egress or new ports. As always, stay current with threats and their detection methods.

Trojan Horse

Dr. Bob's wife really did like playing Whack-A-Mole and it was really difficult to find a copy that wasn't infected. We always check *all* (including management's) computers for freeware because everybody likes something for free, especially when a friend e-mails it to you. Security awareness is the best ROI on fixing this problem. This is a potential reload of the operating system to fully remove the threat. Hey, it's OK because you have a full recent backup, correct?

Although the short-term responses are not earth-shaking events, they could grow into a large mess if not dealt with properly. *Always* monitor the computer in question for a time to verify that there is no residual effect from the incident. Most businesses have no idea where their data is going because they have no egress monitoring. Know where and how much of your data is leaving the facility! The use of an internal honey pot will help you see if there is any strange activity and will also act as an early warning system for other creepy, crawly things on your network.

These are some standard incident management responses to common problems. Constant updating of the management plan will help the team function quicker and with a higher eradication rate.

Distributed Denial of Service

Most people are shocked when they get their first denial-of-service (DoS) attack, the net drrraaaaggggss. Start by checking the firewall logs and you'll see lots of different addresses giving just part of the TCP handshake. This threat can be reduced in the preparation stage by modifying the settings on the router, the Windows connect time, and the response time to the TCP handshake. Most vendors have a how-to on decreasing the threat of distributed DoS (DDoS). This should be a standard part of defense-in-depth hardware hardening. Not if, When.

Theft of Laptop

This is quickly becoming the most common incident management problem. The most important thing is knowing what's on each laptop and is it encrypted? Check VPN logs for activity and any other tracking controls that might be installed. Interview those involved. Note: If you are not trained in interview and interrogation techniques, you can do more damage than good. Misspeaks by the interviewer can give the guilty party more information to reinforce their story. Again, good security awareness can reduce this threat and the extended time needed to manage this incident.

Summary of Incident Management

Short-term incident management events happen frequently, are localized to a very few machines and pose a low threat vector if caught early. Although these aren't the glory jobs some of us like, these are what you'll see the most of. It is basically disconnect → clean → verify → return.

Standard-length incident management responses are actually rare. Major hacker events, like break-ins, are very newsworthy but happen far less than a worm on a computer. These are department or company-wide, affecting multiple machines or involving the theft of records. Decisions on whether to disconnect the computer from the network before forensics can be performed should be seriously considered. Isolation methods using a virtual switch, honey pots, and a packet scanner might help determine what the intended target was (web server, SQL server) and where the data might be going. Some incident management teams immediately unplug the machine in question from the local/Internet and miss the opportunity for live forensics and analysis of the problem. Hey, they got you already, might as well take a few minutes to do some analysis.

Chapter Summary

Computer security incident management is rising in awareness, utilization, and methodologies. Major organizations such as the NIST, DHS, US-CERT, and others have developed methodologies to minimize the effect of a security event. Most of these follow the same path, just described by different words for the same task/job. It really doesn't matter which method you use, just make sure you use an organized methodology that will meet all your organization's needs. Small businesses and enterprises must comply with Federal regulations, and how it's done is where the variations in methodology start to meet each group's needs.

Proper top-down design will help with planning, implementing, and maintaining a productive team. Proper selection of staff and ongoing extensive training is a must as is a functional process with dealing with most computer security events.

Additional Help

ISO
- – 27002: Information Security Management, Chapter 13: Information Security Incident Management

NIST
- – 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- – 800-61: Computer Security Incident Handling Guide
- – 800-83: Guide to Malware Incident Prevention and Handling
- – 800-86: Guide to Integrating Forensic Techniques into Incident Response

- COBIT
  - PO5
  - PO6
  - PO9
- PCI-DSS
  - Requirement 11
  - Requirement 12

Chapter 12

Asset Classification

Thomas R. Peltier and William Tompkins

Contents

Introduction

With the United States Congress on full alert regarding the protection of information assets, and the international community certifying organizations to information security standards, the requirement for an asset classification policy and its supporting procedures remains a top consideration for protecting any organization's information assets. As a security professional, it is important for you to know that an asset or information classification policy is only one element in the overall information management process. In many organizations, a close integration of information recovery priorities, the business impact assessment, and information classification has strengthened management's understanding of both the role and the importance of asset classification. In addition, the information classification policy needs to be coupled with a records management policy.

Any security standard or best practice needs to be founded on a solid foundation of asset classification. To ensure proper protection of our information resources, it is necessary to define what an owner is and how that entity has ultimate responsibility for the information assets within their business unit; this includes the classification and assigning of retention requirements. By implementing an asset management scheme and supporting methodology, we are able to determine the required controls commensurate with the sensitivity of the information as classified by the owner.

In this chapter, we will explore the need for both policies, examine their contents, and then critique some examples.

Overview

As we will discuss later in this chapter, information classification is only one of the elements in an effective information management program. Knowing what we have and how important it is to the organization is the key to the success of the information security program. The implementation of this program will require that representatives of the organization be charged with exercising its proprietary rights. In addition, a full inventory of these assets must be conducted with a requirement for annual review established.

Why Classify Information?

Organizations classify information to establish the appropriate levels of protection for these resources. Because resources are limited, it will be necessary to prioritize and identify what really needs protection. One of the reasons to classify information is to ensure that scarce resources are deployed where they will do the most good. The return on investment for implementing an encryption system to protect public domain information would not be considered a sound business decision. All information is created equal, but not all information is of equal value (Figure 12.1).

Of all of the information found within an enterprise, approximately only 10% of it is actually competitive advantage, trade secret, or personal information. The biggest portion of organization information is information that is typically accessed by most or all employees to do their assigned tasks. The remaining information has been made available to the public through authorized channels. Information resources that are classified as public would include annual stockholders' reports, press releases, and other authorized public announcements.

An effective way of understanding the difference between internal use information and public information is to picture your organization's connection to the Internet. The web site and the information contained on it, which is outside your zone of protection, is your public information. Remember, posting information to the public web site is only done by the web master and with the approval of the owner of the information. This is your organization's Internet connection.

The portion of Internet access that is behind your zone of protection and contains information for use by employees is your Intranet connection. This area contains information that is unavailable to the outside world but has been made accessible to employees for use while performing their assigned tasks.

For years, the information-handling standard was that all information is closed until the owner opens it. This worked well in the mainframe environment when access control packages ruled the single platform of information processing. With the introduction of the client–server environment and the multiple-platforms operating situation, no one access control package could handle all of the needs. With decentralized processing and then the move to connect to the Internet, restrictions on information closure began to weaken. The operating concept during this period was that all information was open until the owner classified it and closed access to it.

Now we have gone full circle. As the decentralized processing environment matures and national and international laws, statutes, and privacy concerns become

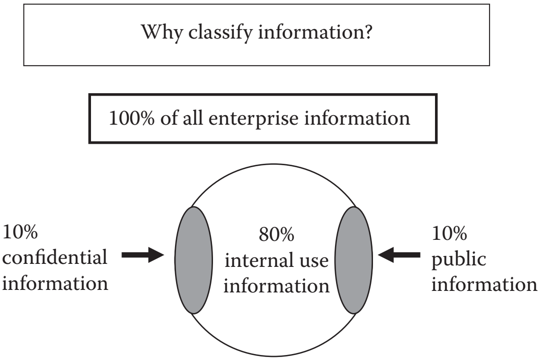

Why classify information?
100% of all enterprise information
10% confidential information
80% internal use information
10% public information

Figure 12.1 Information classification breakdown.

stronger, the information protection concept has reverted to one in which all information access is closed until the owner opens access. For this to be effective, and to allow the organization to demonstrate due diligence, it is incumbent that the organization establish an effective information classification policy and supporting handling standards.

Most organizations do not have information that is all the same value or sensitivity. It is necessary to at least develop an initial high-level attempt at classification. This should be done, if for no other reason, to ensure that budgeted resources are not misused in overprotecting nonsensitive/noncritical information assets. Before employees can protect information assets, they must first have a policy that identifies classification levels and then a methodology to implement the policy requirements. An information classification policy that is not overly complex and a methodology that relies on common sense and is facilitated by either information security or records management will make acceptance possible.

What Is Information Classification?

An asset or information classification process is a risk-based business decision process with consideration of legal/regulatory compliance. Information is an asset of the organization and management is charged with protecting and accounting for proper use of all assets. An information classification process will allow managers to meet this fiduciary responsibility. The role of the information security professional or even that of information systems personnel is one of advice and consulting. The final decision is made by the business unit managers or, as we have defined, the asset owner.

When preparing to develop the information classification policy, it is essential to get input from the management team. It is important that you ask questions to find out what they mean. When my daughter was about 7 or 8 years old, she came to me and asked, "Pa (that what she calls me), where do we come from?" Well, I pretended to not hear her so I could research my answer. The next day I sat down with her and discussed the "facts of life" with her. She looked at me and said, "I know all that. What I want to know is where we come from. Terri Lynn comes from Tennessee and Pam comes from Kentucky." So, before you develop an answer, make sure you understand the question.

When conducting interviews with management and other key personnel, develop a set of questions to ensure consistency in the direction of the responses. These questions might include some of the following:

- What are the mission-critical or sensitive activities or operations?
- Where is mission-critical or sensitive information stored?
- Where is this information processed?
- Who requires access to this information?

There are no hard-and-fast rules for determining what constitutes sensitive information. In some instances, the number of people who require access may affect the classification. The real test of an information classification system is how easy it is for the reader to understand what constitutes sensitive information and what organization-approved label should be affixed to the information asset resource.

Where to Begin?

After you have a clearer idea of what management is expecting, it is time to do some research. I like to contact my fellow information security professionals and find out what they have done to answer the problems I have been assigned. By being a Certified Information Systems Security Professional (CISSP) and also being a member of the Information System Security Association (ISSA) and the Information Systems Audit and Control Association (ISACA), I have a ready access to people in my area that are usually willing to share examples of their work.

When developing classification levels, I prefer to discuss the topic with fellow professionals. I recommend that you cultivate contacts in similar business environments and see what your peers are doing. The Internet can generate some examples of classification policies, but many of them are university-related or government agency–related. Be careful of what you uncover in your research, although there are many good ideas and terms out there, they are only good if they are applicable to your specific needs.

Use the information you gather from fellow professionals as a starting point. Your organization will have its own unique variation on the classification policy and categories. We will examine a number of examples of information categories. If you are a government agency, or do work for a government agency, be sure to check with your regulatory affairs group to determine if there are any government-imposed requirements.

Examples

As a starting point in a classification scheme, a company can include a mechanism to establish the criticality of information. This scheme established three information classification categories (Figure 12.2a) and now adds four impact categories (Figure 12.2b). Using these sets of definitions, the manager of the information resources will be able to determine how critical the asset is to the company (Figure 12.3).

In Example 2, the service provider has established five categories to be used by managers in classifying information assets. Part of the reason for their use of these categories is that they have experience with Department of Defense contracts and have become used to certain classification levels. The concern I have with patterning a policy after a government standard is that there may be confusion as to what government contact information is and what normal business information is. Also, the number of employees exposed to the government standards might affect the drafting of these standards (Figure 12.4).

(a) **Mega oil corporation**

Highly confidential—information whose unauthorized disclosure will cause the corporation severe financial, legal, or reputation damage. Examples: acquisitions data, bid details, and contract negotiation strategies.

Confidential—information whose unauthorized disclosure may cause the corporation financial, legal, or reputation damage. Examples: employee personnel and payroll files, competitive advantage information.

General—information that, because of its personal, technical, or business sensitivity, is restricted for use within the company. Unless otherwise classified, all information within Mega Oil Corporation is in this category.

(b) **Impact categories**

Maximum—information whose unauthorized modification and destruction will cause the company severe financial, legal, or reputation damage.

Medium—information whose unauthorized modification and destruction may cause the company financial, legal, or reputation damage. Examples: electronic funds transfer, payroll, and commercial checks.

Minimum—although an error in this data would be of minimal consequence, this is still important company information and therefore will require some minimal controls to ensure a minimal level of assurance that the integrity of the data is maintained. This applies to all data that is not placed in one of the above classifications. Examples: lease production data, expense data, financial data, and exploration data.

Critical—it is important to assess the availability requirements of data, applications, and systems. A business decision will be required to determine the length of unavailability that can be tolerated before expending additional resources to ensure the information availability that is required. Information should be labeled "critical" if it is determined that special procedures should be used to ensure its availability.

Figure 12.2 Information classification categories (a) and impact categories (b). (Example no. 2).

1 – Availability safeguards must be implemented
2 – Availability safeguards should be implemented
3 – Continue to monitor availability requirements
4 – No additional action required as this time

		Classification level		
		Highly confidential	Confidential	General
Business impact	Maximum	1	2	3
	Medium	2	2	3
	Minimum	2	3	4

Figure 12.3 Criticality matrix.

International service provider

Top secret—information that, if disclosed, could cause severe effects on the company's competitive advantage or business strategies

Confidential—information that, if disclosed, could violate the privacy of individuals, reduce competitive advantage, or damage the company

Restricted—information that is available to a specific subset of the employee population when conducting company business

Internal use—information that is intended for use by all employees when conducting company business

Public—information that has been made available to the public through authorized company channels

Figure 12.4 Information classification category (Example no. 2).

I recently discussed this classification scheme with the company that created it to find out how they could use a color-coding scheme (Figure 12.5). The company does not actually use the colors to color-code the documents. Instead, the company identifies the level of classification but requires that the footer contain "Company Red" or whatever color. It gives a good visual for the employees.

The company also requires that specific levels of information contain appropriate markings to identify it as classified information (Figure 12.6). We will be

Global manufacturer

Company confidential red—provides a significant competitive advantage. Disclosure would cause severe damage to operations. Relates to or describes a long-term strategy or critical business plan. Disclosure would cause regulatory or contractual liability, severe damage to our reputation or the public image, severe loss of market share or the ability to be first to market; the loss of an important customer, shareholder, or business partner, or a long-term or severe drop in stock value. There is a strong likelihood that somebody is seeking to acquire this information.

Company confidential yellow—provides a competitive advantage. Disclosure could cause moderate damage to the company or an individual. Relates to or describes an important part of the operational direction of the company over time. Provides important technical or financial aspects of a product line or a business unit. Disclosure could cause a loss of customer or shareholder confidence, or could cause a temporary drop in stock value. Very likely that some third party would seek to acquire this information.

Company confidential green—might provide a business advantage over those who do not have access to the same information. Might be useful to a competitor. Not easily identifiable by inspection of a product. Not generally known outside of the company or available from public sources. Generally available internally. Little competitive interest.

Company public—would not provide a business or competitive advantage. Routinely made available to interested members of the general public. Little or no competitive interest.

Figure 12.5 Information classification category (Example no. 3).

Company confidential—a subset of Company Internal information, the unauthorized disclosure or compromise of which would likely have an adverse effect on the company's competitive position, tarnish its reputation, or embarrass an individual. Examples: customer, financial, pricing, or personnel data; merger/acquisition, product, or marketing plans; new product designs, proprietary processes, and systems.

Company internal—all forms of proprietary information originated or owned by the Company, or entrusted to it by others. Examples: organization charts, policies, procedures, phone directories, and some types of training materials.

Company public—information officially released by the company for widespread public disclosure. Example: press releases, public marketing materials, employment advertising, annual reports, product brochures, the public web site, etc.

Figure 12.6 Information classification category (Example no. 4).

discussing an information-handling matrix later in this chapter. When you create your organization's handling requirements, use the following as thought starters:

- Make no copies
- Third-party confidential
- Attorney–client privileged document
- Distribution limited to (…)
- Covered by a nonanalysis agreement

Resist the Urge to Add Categories

Keep the number of information classification categories to as few as possible. If two possible categories do not require substantially different treatments, then combine them. The more categories that are available, the greater the chance for confusion among managers and employees. Normally, three or four categories should be sufficient to meet your organizations' needs.

Additionally, avoid the impulse to classify everything the same. To simplify the classification process, some organizations have flirted with having everything classified as confidential. The problem with this concept is that confidential information requires special handling. This would violate the concept of placing controls only where they are actually needed. This method would require the organization to waste limited resources protecting assets that do not really require that level of control.

Another pitfall to avoid is to take the information classification categories developed by another enterprise and adopt them verbatim as your own. Only use the information created by other organizations to assist in the creation of your organization's unique set of categories and definitions.

In some government sectors, there are five categories for information classification (top secret, secret, confidential, restricted, and unclassified). In addition to the categories, there are additional impact levels of sensitive and nonsensitive. Using this scheme, it would be possible to have an information asset of higher concern if it is classified *restricted/sensitive* compared with one that was classified co*nfidential/nonsensitive*. In addition, information labeled as *unclassified* has the classification level of unclassified, so it has actually been classified. Sometimes, I think Joseph Heller, in *Catch 22*, actually established a guideline for government and industry to use when developing standards and policies.

What Constitutes Confidential Information

There are a number of ways to look at information that may be classified as confidential. We will examine a number of statements relating to confidential information. The first is a general statement about sensitive information:

For a general definition on what might constitute confidential information, it may be sufficient to define such information as

> Information that, if disclosed, could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the organization.

The Economic Espionage Act (EEA) of 1996 defines "trade secret" information to include "all forms and types of financial, business, scientific, technical, economic, or engineering information" regardless of "how it is stored, compiled or memorialized." The EEA criminalizes the actions of anyone that

- Steals or, without authorization, appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret
- Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret
- Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization
- Conspires with one or more other persons to commit any offense described in any the EEA under the heading "conspiracy"

There are a number of other information classification types that you may have heard about over the years. Let's take just a minute to review copyrights, patents, and trademarks.

Copyrights—at regular intervals, employees will be creating new work in the form of application programs, transactions, systems, web sites, and so forth. To protect the organization from loss of created material enterprise, policies on copyright ownership must be implemented and all employees must be reminded of these policies on a regular basis. This is typically established in a "Terms of Employment" document that is reviewed by all employees and re-certified annually.

Unlike other forms of intellectual property protection, the basis for copyright occurs at the creation of an original work. Although copyrights are granted by government copyright offices; every original work has an inherent right to a copyright and is protected by that right even if the work is not published or registered.

All original works of authorship created by employees for a company are the property of the company and are protected by the copyright law. The copyright also applies to consultants doing work for your organization while under a purchase order or other contractual agreement. Unless there is an agreement to the contrary, any work created by a contractor under contract to an organization is owned by the organization, not the contractor.

The types of work that qualify for copyright protection include

- All types of written works
- Computer databases and software programs (including source code, object code, and micro code)
- Output (including customized screens and printouts)
- Photographs, charts, blueprints, technical drawings, and flowcharts
- Sound recordings

A copyright does not protect

- Ideas, inventions, processes, and three-dimensional designs (these are covered by *Patent Law*)
- Brands, products, or slogans (which are covered by *Trademark Law*)

The information classification policy that you will be developing will discuss the organization's confidential information. Typically, this type of information will consist of either competitive advantage/trade secret information or personal information.

The laws regarding trade secret information were developed from the duty of good faith generally imposed in commercial dealings. A trade secret is commonly defined as information deriving actual or potential economic value by virtue of its not being readily ascertainable through proper means by the public, and which is the subject of reasonable efforts to maintain its secrecy. The legal system protects the owner (in our case, the organization) from someone who uses improper means to learn trade secrets, either directly or indirectly. Therefore, anyone using improper means to learn trade secrets has breached a duty of good faith in dealing with the trade secret's owner.

The breach of that duty of good faith usually takes the form of an abuse of a confidence, the use of improper means to ascertain the secret, or a breach of contract. Anyone involved in the breach of that duty is liable for trade secret stealing.

The laws and requirements governing trade secret and competitive advantage information are well established and offer substantial penalties for noncompliance. The area of personal information has reached a new level of importance with businesses/governments and their customers/constituents. Organizations now routinely refer to the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLBA), European Union privacy laws, and the Payment Card Industry Data Security Standard (PCI DSS) when establishing safeguards in their business processes and for protecting personal information.

Any policy and supporting standards on information classification levels must take into account not only the trade secret and competitive advantage information but must also include any personal information about employees, customers, clients, and other third parties.

Earlier in this chapter, we examined a number of examples of information classification categories. Now, we will discuss one other important element, the role of employees in the information classification process.

Employee Responsibilities

When I was doing research for this section of the book, I came across the following policy statement:

> The "Information Owner" means the party who *confides* the referenced *confidential information* to the other party, the *confidant*. Despite the name, the information owner benefits from a *confidentiality engagement* with respect to *confidential information* that it owns or possesses.

These two sentences have five terms that require the reader to get further definitions. As I attempted to determine exactly what it means to "confide," I was sent to a hypertext page that explained that it meant to "entrust" the information to a "confident," which means the "party receiving the information," and at that point, I started looking elsewhere for examples.

The two-sentence policy above is a good example of what should be avoided when you are writing a policy, or writing anything regarding information security. The document we just referenced came from an organization with strong roots in the legal and government sector. If this is your audience, than this is the language for you. If not, try to think like Henry David Thoreau and "simplify."

There are typically three areas of employee responsibility: owner, user, and custodian. Some organizations are adding and documenting a governance role, that of the "steward"—these policy people (executive and senior level managers) have responsibilities that include data governance policies, advising owners and managers on the implementation of policies, and defining performance measures to help determine how well data governance is working. With that "addition" noted, we will explain each of the three primary concepts (owner, user, and custodian) and examine how other organizations have defined these responsibilities.

Owner

The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization's proprietary rights, define access criteria requirements and direct custodians to provide access privileges to those with a true business need. This role is normally assigned to the senior level manager within the business unit where the information asset was created or is the primary user of that asset. The manager will have the ultimate responsibility for compliance, but they will probably delegate the day-to-day activities to some individual that reports to them.

> Information owner—the person who creates or initiates the creation or storage of the information is the initial owner. In an organization, possibly with divisions, departments, and sections, the owner becomes the unit itself, with the person responsible being designated "head" of the unit.
>
> The information owner is responsible for ensuring that
>
> - A classification hierarchy is agreed upon and that this is appropriate for the types of information processed for that business unit.
> - Classify all information stored into the agreed upon types and create an inventory (listing) of each type.
> - For each document or file within each classification category, append its agreed upon (confidentiality) classification. Its availability should be determined by the respective classification.
> - Ensure that, for each classification type, the appropriate level of information security safeguards are available, for example, the log-on controls and access permissions applied by the information custodian provide the required levels of confidentiality.
> - Periodically, check to ensure that information continues to be classified appropriately and that the safeguards remain valid and operative.

I am not certain what being designated "head" actually means, but I don't believe I would want that title. The term "initial owner" may also lead the reader to believe that someone else may come along and become the "final" or "ultimate" leader.

We will now review the owner definition from a global media organization.

> Owners are authorized employees to whom responsibility has been delegated for the creation and/or use of specific business data by the

> business unit, which "owns" the data. Owners are responsible for defining requirements for safeguards that assure the confidentiality, availability, and integrity of the information. Owners are also responsible for placing information in the proper classification so that those who need the information to perform their assigned duties can obtain it. The owner provides requirements for security for the information to the custodian. The custodian implements the controls to meet the owner's requirements.

This is a fairly good definition. The only element that I might add is the requirement that the owner monitor the safeguards to ensure custodian compliance. Let's examine one more example.

> A. *Owner*: the company management of an organizational unit, department, etc., where the information is created, or that is the primary user of the information. *Owners* have the responsibility to
>
> 1. Identify the classification level of all corporate information within their organizational unit
> 2. Define and implement appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource
> 3. Monitor safeguards to ensure their compliance and report situations of noncompliance
> 4. Authorize access to those who have a business need for the information
> 5. Remove access from those who no longer have a business need for the information

We will be seeing variations on this definition in the following section.

Custodian

The next responsibility we will have to create is that of the information custodian. This entity is responsible for implementing information technology processes to control access (or access levels) for protecting the information asset based on the requirements established by the owner. In an organization that has an information systems organization, the operations group might be considered the custodian of client data and information. They do not have the right to permit anyone access to the information asset until access criteria is specified by the owner, nor can they alter the information in any way without approval from the owner. This would include any programming or system upgrades that would modify the information or the output from applications and transactions.

> An Information Custodian is the person responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the Information Owner.
>
> This could be the System Administrator controlling access to a computer network, a specific application program, or even a standard filing cabinet.

This example started out well, but finished oddly. Giving examples of what might be considered to be a custodian is good. Trying to link a filing cabinet to the opening sentence where the policy identifies the custodian as a "person." Remember, when you are writing, go back and read what you just wrote to make sure the concepts match from beginning to end. Don't try to be cute. Stick to what the subject is and make sure you say exactly what needs to be said.

> Custodians are authorized system support persons or organizations (employees, contractors, consultants, vendors, etc.) responsible for maintaining the safeguards established by owners. The owner designates the custodian. The Custodian is the "steward of the data" for the owner, i.e., the Data Center may be the Custodian for a business application "owned" by a Business Unit.

The use of the term "steward of the data" brings out a point that needs to be made. Some organizations and cultures prefer other terms than the ones discussed here. When I was younger, I played Pony League baseball for a team called the "Custodians," which was funded by the Roseville Public Schools maintenance staff. Our uniforms looked more like big league uniforms because we had the name on the front and number on the back. The other teams had names like "Tigers" and "Braves" but had some advertisement about their sponsor on the back. It wasn't until we played a few games that the other teams started calling us The Janitors. Custodian to some is a noble name; to others, maybe not so noble. So choose your terms wisely. Curator, keeper, and guardian are other terms that might work.

In the past, we were doing work for HIPAA compliance while developing policies for a hospital. When we discussed the definition for "user," the hospital staff started to chuckle and told us that the term "user" had a totally different meaning there and we needed to find another term.

> B. *Custodian*: employees designated by the owner to be responsible for maintaining the safeguards established by the owner.

It is important to remember that when we use the term "employee," we are actually discussing the virtual employee. We can only write policy for employees;

for all third parties, a contract must contain compliance language. So it is perfectly acceptable to identify "employees" even if we know that someone other than an employee may actually perform the function. This is true for all employee responsibilities except "owner." The owner must be an employee; after all, it is the organization's information.

User

The final element is the user and this individual is granted permission to access the information asset by the owner. They are to use the information in the manner agreed upon with the owner. They have no other rights. When granting access, the owner should use the concept of "least privilege." This means that the user is granted only the access they specifically need to perform their business task and no more.

> An Information User is the person responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the Information Owner.

The inventory discussed here will be addressed in both the classification policy and the records management policy. Including who has been assigned access and who needs to be tracked. The Custodian is generally responsible for providing the tools to monitor the user list.

> Users are authorized system users (employees, contractors, consultants, vendors, etc.) responsible for using and safeguarding information under their control according to the directions of the Owner. Users are authorized access to information by the Owner.

The final example is similar to the definition used above.

> C. *User*: Employees authorized by the Owner to access information and use the safeguards established by the Owner.

Classification Examples

In this section, we will examine the attributes and examples of different classification categories. We will also present examples of organization information classification policies.

Information classification

Policy: security classifications should be used to indicate the need and priorities for security protection

Objective: to ensure that information assets receive an appropriate level of protection

Statement: information has varying degrees of sensitivity and criticality. Some items may require an additional level of security protection or special handling. A security classification system should be used to define an appropriate set of security protection levels, and to communicate the need for special handling measures to users

Figure 12.7 Information classification policy (Example no. 1).

Critique of Example No. 1—this is an actual classification policy (very high level) for the executive branch of a national government (Figure 12.7). There is little here to help the average user. This is an example of a program or general policy statement; however, a topic-specific policy statement may have been more beneficial. Perhaps the next two examples will provide more information.

Critique of Example No. 2—the policy seems to stress competitive advantage information in its opening paragraphs (Figure 12.8). It does not seem to address personal information about employees or customers. It does provide for these topics as categories under *Confidential* but it never really mentions them by name. This seems to be a policy that is somewhat limited in scope. Additionally, it does not establish the scope of the information (is it computer-generated only or exactly what information is being addressed). The employee responsibilities are missing. What is management's responsibility with respect to information classification, and what is expected of the employees? Finally, what are the consequences of noncompliance?

Critique of Example No. 3—Examples 2 and 3 are very similar, this one does address the role of the Owner, but it fails to define what an Owner is (Figure 12.9). The issue of noncompliance is not addressed and the scope of the policy is vague.

Classification requirements

Classified data is information developed by the organization with some effort and some expense or investment that provides the organization with a competitive advantage in its relevant industry and that the organization wishes to protect from disclosure.

Although defining information protection is a difficult task, four elements serve as the basis for a classification scheme:

1. The information must be of some value to the organization and its competitors so that it provides some demonstrable competitive advantage.
2. The information must be the result of some minimal expense or investment by the organization.
3. The information is somewhat unique in that it is not generally known in the industry or to the public or may not be readily ascertained.

Figure 12.8 Information classification policy (Example no. 2).

4. The information must be maintained as a relative secret, both within and outside the organization, with reasonable precautions against disclosure of the information. Access to such information could only result from disregarding established standards or from using illegal means.

Top secret (secret, highly confidential)

Attributes:

- Provides the organization with a very significant competitive edge
- Is of such a nature that unauthorized disclosure would cause severe damage to the organization
- It shows specific business strategies and major directions, and
- Is essential to the technical or financial success of a product

Examples:

- Specific operating plans, marketing strategies
- Specific descriptions of unique parts or materials, technology intent statements, new technologies and research
- Specific business strategies and major directions

Confidential (sensitive, personal, privileged)

Attributes:

- Provide the organization a significant competitive edge
- Is of such a nature that unauthorized disclosure would cause damage to the organization
- It shows operational direction over an extended period
- Is extremely important to the technical or financial success of a product

Examples:

- Consolidated revenue, cost, profit, or other financial results
- Operating plans and marketing strategies
- Descriptions of unique parts or materials, technology intent statements, new technological studies and research
- Market requirements, technologies, product plans, revenues

Restricted (internal use)

Attributes:

- All business-related information requiring baseline security protection, but failing to meet the specified criteria for higher classification
- Information that is intended for use by employees when conducting company business

Examples:

- Business information
- Organization policies, standards, procedures
- Internal organization announcements

Public (unclassified)

Attributes:

- Information which, due to its content and context, requires no special protection, or
- Information which has been made available to the public distribution through authorized company channels

Examples:

- Online public information, web site information
- Internal correspondences, memoranda, and documentation which do not merit special controls
- Public corporate announcements

Figure 12.8 (Continued) Information classification policy (Example no. 2).

Information classification

Introduction
Information, wherever it is handled or stored (for example, in computers, file cabinets, desktops, fax machines, voice mail) needs to be protected from unauthorized access, modification, disclosure, and destruction. All information is *not* created equal. Consequently, segmentation or classification of information into categories is necessary to help identify a framework for evaluating the information's relative value and the appropriate controls required to preserve its value to the company.

Three basic classifications of information have been established. Organizations may define additional subclassifications as necessary to complete their framework for evaluating and preserving information under their control.

When information does require protection, the protection must be consistent. Often, strict access controls are applied to data stored in the mainframe computers but are not applied to office workstations. Whether in a mainframe, client server, workstation, file cabinet, desk drawer, waste basket, or in the mail, information should be subject to appropriate and consistent protection.

The definitions and responsibilities described below represent the minimum level of detail necessary for all organizations across the company. Each organization may decide that additional details are necessary to adequately implement information classification within their organization.

Corporate Policy:
All information must be classified by the *owner* into one of three classifications: *Confidential*, *Internal Use*, or *Public*.

Confidential
Definition: Information which, if disclosed, could

- Violate the privacy of individuals
- Reduce the company's competitive advantage, or
- Cause damage to the company

Examples: Some examples of *Confidential* information are

- Personnel records (including name, address, phone, salary, performance rating, social security number, date of birth, marital status, career path, number of dependents, etc.)
- Customer information (including name, address, phone number, energy consumption, credit history, social security number, etc.)
- Shareholder information (including name, address, phone number, number of shares held, social security number, etc.)
- Vendor information (name, address, product pricing specific to the company, etc.)
- Health insurance records (including medical, prescription, and psychological records)
- Specific operating plans, marketing plans, or strategies
- Consolidated revenue, cost, profit, or other financial results that are not public record
- Descriptions of unique parts or materials, technology intent statements, or new technologies and research that are not public record
- Specific business strategies and directions
- Major changes in the company's management structure, and
- Information that requires special skills or training to interpret and employ correctly, such as design or specification files

If any of these items can be found freely and openly in public records, the company's obligation to protect from disclosure is waived.

Figure 12.9 Information classification (Example no. 3).

Internal Use

Definition: Classify information as *Internal Use* when the information is intended for use by employees when conducting company business.

Examples: Some examples of *Internal Use* information are

- Operational business information/reports
- Non–company information that is subject to a nondisclosure agreement with another company
- Company phone book
- Corporate policies, standards, and procedures, and
- Internal company announcements

Public

Definition: Classify information as *Public* if the information has been made available for public distribution through authorized company channels. Public information is not sensitive in context or content, and requires no special protection.

Examples: The following are examples of *Public* information:

- Corporate Annual Report
- Information specifically generated for public consumption such as public service bulletins, marketing brochures, and advertisements

Figure 12.9 (Continued) Information classification (Example no. 3).

Critique of Example No. 4—the intent of the policy is that "Information is a corporate asset and is the property of the Corporation." The scope of the policy is "Corporate information includes electronically generated, printed, filmed, typed, or stored data." The responsibilities are well established. The issue of compliance is the only policy element that seems to be lacking (Figure 12.10).

Declassification or Reclassification of Information

Part of an effective information classification program is the ability to combine the requirements with a Records Management Policy. Information assets must be protected, stored, and then destroyed based on a policy and a set of standards. The information classification policy will ensure that an owner will be assigned to each asset, that a proper classification will be assigned, and that an information-handling set of standards will help in the control of copies.

The records management policy will require that the owner provide a brief description of the information record and the record retention requirements. These requirements will be a set of standards that support the records management policy. We will now take a few minutes to examine what is typically part of a records management policy.

Information management

1. General

   A. Corporate information includes electronically generated, printed, filmed, typed, or stored

   B. Information is a corporate asset and is the property of the Corporation

2. Information retention

   A. Each organization shall retain information necessary to the conduct of business

   B. Each organizational unit shall establish and administer a records management schedule in compliance with applicable laws and regulations, and professional standards and practices, and be compatible with Corporate goals and expectations

3. Information protection

   A. Information must be protected according to its sensitivity, criticality and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed.

   B. Employees are responsible for protecting corporate information from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. To facilitate the protection of corporate information, employees' responsibilities have been established at three levels: *Owner, Custodian*, and *User*.

      1. *Owner*: Company management of the organizational unit where the information is created, or management of the organizational unit that is the primary user of the information. *Owners* are responsible for

         a. Identifying the classification level of all corporate information within their organizational unit

         b. Defining appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource

         c. Monitoring safeguards to ensure they are properly implemented

         d. Authorizing access to those who have a business need for the information, and

         e. Removing access from those who no longer have a business need for the information

      2. *Custodian*: Employees designated by the owner to be responsible for maintaining the safeguards established by the owner

      3. *User*: Employees authorized by the owner to access information and use the safeguards established by the owner

   C. Each Vice President shall appoint an Organization Information Protection Coordinator who will administer an information protection program that appropriately classifies and protects corporate information under the Vice President's control and makes employees aware of the importance of information and methods for its protection

4. Information classification

   To ensure the proper protection of corporate information, the owner shall use a formal review process to classify information into one of the following classifications:

   A. *Public*: Information that has been made available for public distribution through authorized company channels. (Refer to Communication policy for more information

   B. *Confidential*: Information that if disclosed, could violate the privacy of individuals, reduce the company's competitive advantage, or could cause significant damage to the company

   C. *Internal Use*: Information that is intended for use by all employees when conducting company business. Most information used in the company would be classified internal use

Figure 12.10 Information classification policy (Example no. 4).

Records Management Policy

An organization's records are one of its most important and valuable assets. Almost every employee is responsible for creating or maintaining organization records of some kind, whether in the form of paper, computer data, optical disk, electronic mail, or voice mail. Letters, memoranda, and contracts are obviously information records, as are things such as a desk calendar, an appointment book, or an expense record.

Organizations are required by law to maintain certain types of records, usually for a specified time. The failure to retain such documents for these minimum periods can subject an organization to penalties, fines, or other sanctions or could put it at a serious disadvantage in litigation. Therefore, every organization should implement a Record Management Policy to provide standards for maintaining complete and accurate records to ensure that employees are aware of what records to keep and for how long; what records to dispose of, and how to dispose of them.

The cost of storage and the administration problems involved in retaining material beyond its useful life are a few important reasons to establish a Records Management Policy. Consideration should also be given to the effect that a failure to produce subpoenaed records might have on the organization when defending itself against a lawsuit. Determining the proper retention periods for information records is a requirement in today's operating environment. Information records should be kept only as long as they serve a useful purpose or until legal requirements are met. At the end of the retention period, records should be destroyed in a verifiable manner. Implementing effective information classification and records management policies makes sound business sense and shows that management is practicing its due diligence.

Before drafting a record management policy, consult with your legal staff to ensure that the policy reflects any relevant statutes. The retention standards that support the policy should be reviewed annually when an information asset inventory is conducted organization-wide (Figure 12.11).

Information-Handling Standards Matrix

Because information classification and records management are unique in their standards requirements, I thought it appropriate to give examples of what these standards might look like. When you are developing your policies, use these as guidelines, not as the standards:

- Printed material (Figure 12.12)
- Electronically stored information (Figure 12.13)
- Electronically transmitted information (Figure 12.14)
- Record management retention schedule (Figure 12.15)

Record management policy

Introduction

It is the policy of the Company to accommodate the timely storage, retrieval, and disposition of records created, utilized, and maintained by the various departments. The period of time that records are maintained is based on the minimum requirements set forth in State and Federal retention schedules.

1. **Role of the Retention Center**

   The role of the Retention Center is to receive, maintain, destroy, and service inactive records that have not met their disposition date. Each business unit is to establish schedules to comply with the minimum amount of time records should be maintained in compliance with State and Federal guidelines. Retention requirements apply whether or not the records are transferred to the Retention Center. Copies of the schedules must be maintained by the business unit and available for inspection.
2. **Role of the Records Manager**

   The role of the Records Manager is to administer the Records Management program. The Records Manager is well acquainted with all records and/or record groups within an agency and has expertise in all aspects of records management. The duties of the Records Manager include planning, development, and administration of records management policies. These duties also include the annual organization-wide inventory of all information assets to be conducted by the Business Unit Manager with reports sent to the Records Manager.
3. **Role of Management Personnel**

   Management Personnel are responsible for records under their control.
4. **Role of Departmental Records Coordinator**

   The Departmental Records Coordinator is to be a liaison between the department and the Retention Center. It is recommended that each department appoint a Records Coordinator in writing. The letter of appointment should include the Records Coordinator's full name, department, and telephone extension. The letter should be forwarded to the Retention Center and maintained on file.
5. **Type of Documents Maintained in Retention Center**

   5.1. Record Retention accepts only public records that are referenced in the State Retention Schedule, except student transcripts. Copies of student transcripts may be obtained from Records and Admissions located at the Student Service Center.

   5.2. Record Retention does not accept personal, active, or nonrecords.

   5.3. Record Retention stores only inactive and permanent records until final disposition according to State and Federal retention schedules. Examples include personnel files, purchase orders, grade books, or surveys.

   5.4. Record Retention receives and stores inactive permanent records from TVI departments until final disposition according to State and Federal retention guidelines.

   5.5. Record Retention ensures records are classified according to State and retention guidelines.

   5.6. Record Retention ensures records are tracked and entered into an electronic records management software system, which tracks record boxes, assigns retention schedules, permanent box numbers, destruction dates, and shelf locations.
6. **Services**

   6.1. If a department has obsolete records that are deemed confidential or sensitive, or copies of nonrecords, a special request for shredding may be sent to the Record Retention Center. The records can be shredded by the Record Retention Center staff or transferred to the State Record Center for destruction.

Figure 12.11 Sample record management policy.

6.2. Departments must complete a Request for Destruction form for confidential or nonrecords to be shredded. Departments are required to purchase forms from Central Stores at Shipping and Receiving.

6.3. The Record Retention Center provides consulting services to departments on filing systems and maintenance of records.

7. Transferring Records

7.1. Departments should transfer records to Record Retention for storage in January, July, and October.

7.2. Records with a retention period of 2 years or more should be transferred to Record Retention.

8. Record Retrieval

8.1. Records are retrieved and delivered to customers by request given a 24-hour notice.

8.2. Records can be retrieved for customers on an emergency basis as requested.

8.3. Management personnel, records coordinator, or the requester will sign for receipt of records. Records are to be checked out for no longer than 30 days. If a longer period is required, a written request should be sent to the Retention Center. If records are checked out for more than a year, the records will be permanently withdrawn from inventory.

8.4. Permanent withdrawal: if a department wishes to withdraw a record permanently from storage, forward a request to Record Retention by phone, fax, or interoffice mail. The department will complete a Withdrawal Request form and the records will be deleted from inventory.

8.5. Second Party Withdrawal: if a department requests a record originating from another department, then the requesting department must contact the department of origin to obtain authorization. The department of origin will contact Record Retention for records withdrawal. The department requester must view the requested records at the Record Retention Center.

8.6. Records should not be returned via interoffice mail due to the confidential nature of the documents.

9. Record Destruction

9.1. Record Retention destroys records, according to State guidelines, in January, July, and October.

9.2. Records are destroyed by Record Retention according to State and Federal guidelines when legal requirements are met. A Destruction Request form will be sent to the originating department for review and signature by the Departmental Records Coordinator and by management personnel. Only when the Destruction Request has been reviewed, signed, and returned to Record Retention will the expired records be destroyed. Authorized personnel will shred confidential records. If departments wish to keep the records past their assigned destruction date, management personnel can extend the date for no longer than 1 year unless a litigation, audit, or investigation is pending. Records kept by the department past the retention date of destruction will be permanently withdrawn from the inventory.

9.3. All records scheduled for destruction are reviewed by the Institute's Records Manager and by State Records Analysts for approval.

10. Supplies

10.1. Records must be stored in the appropriate record retention boxes, which are obtained from Central Stores at Shipping and Receiving.

10.2. Storage Ticket forms and Request for Destruction forms are obtained from Central Stores at Shipping and Receiving.

Figure 12.11 (Continued) Sample record management policy.

	Confidential	**Internal Use**	**Public**
Labeling of documents	Document should identify *owner* and be marked "*confidential*" on cover or title page	No special requirements	Document may be marked "*public*" on cover or title page
Duplication of documents	Information *owner* to determine permissions	Duplication for business purposes only	No special requirements
Mailing of documents	No classification marking on external envelope; "*confidential*" marking on cover sheet; confirmation of receipt at discretion of information *owner*	Mailing requirements determined by information *owner*	No special requirements
Disposal of documents	*Owner* observed physical destruction beyond ability to recover	Controlled physical destruction	No special requirements
Storage of documents	Locked up when not in use	Master copy secured against destruction	Master copy secured against destruction
Read access to documents	*Owner* establishes *user* access rules; generally highly restricted	*Owner* establishes *user* access rules; generally widely available	No special requirements; generally available within and outside company
Review of document classification level	Information *owner* to establish specific review date (not to exceed 1 year)	Information *owner* to review at least annually	No special requirements

Figure 12.12 Information-handling matrix for printed material.

Authorization for Access

To establish a clear line of authority, some key concepts will have to be established. As discussed previously, there are typically three categories of employee responsibilities. Depending on the specific information being accessed, an individual may fall into more than one category. For example, an employee with a desktop workstation becomes the owner, custodian, and user. To help better understand the concepts, the responsibilities of each category are listed below.

	Confidential	**Internal use**	**Public**
Storage on fixed media (access controlled)	Unencrypted	Unencrypted	Unencrypted
Storage on fixed media (not access controlled)	Encrypted	Unencrypted	Unencrypted
Storage on removable media	Encrypted	Unencrypted	Unencrypted
Read access to information (includes duplication)	Information *owner* to authorize individual *users*	Information *owner* to define permissions on *user*, group or function basis	No special requirements
Update access to information	Information *owner* to authorize individual *users*	Information **owner** to define permissions on *user*, group or function basis	Information *owners* to define permissions
Delete access to information	Information *owner* to authorize individual *users*; *user* confirmation required	Information *owner* to define permissions on *user*, group or function basis; **user** confirmation required	Information *owner* to define permissions
Print hard copy report of information	Output to be routed to a pre-defined, monitored printer	Information *owner* to define permissions	No special requirements
Internal *labeling* of information at the application or screen/display level	Notification of "*confidential*" to appear at top of display	No special requirements	Notification of "*public*" may optionally appear at top of display
External *labeling* of exchangeable media	Media must identify owner and be marked *confidential*	Marking at discretion of *owner*	No special requirements
Disposal of electronic media (diskettes, tapes, hard disks, etc.)	*Owner* observed physical destruction beyond ability to recover	Physical destruction	No special requirements
Disposal of information	Delete by fully writing over information	Delete files through normal platform delete command, option or facility	No special requirements
Review of classified information for reclassification	Information **owner** to establish specific review date (not to exceed 1 year)	Information *owner* to review annually	Information *owner* to review annually

Figure 12.13 Information-handling matrix for electronically stored information.

	Confidential	Internal use	Public
Logging access activity	Log all access attempts; information *owner* to review all access and violation attempts	Log all violation attempts; information *owner* reviews as appropriate	No special requirements
Access report retention requirements	Information *owner* to determine retention of access logs (not to exceed 1 year)	Information *owner* to determine retention of violation logs (not to exceed 6 months)	No special requirements

Figure 12.13 (Continued) Information-handling matrix for electronically stored information.

By FAX	Attended at receiving FAX	Information *owner* to define requirements	No special requirements
By WAN	Confirmation of receipt required; encryption optional	No special requirements; encryption optional	No special requirements
By LAN	Confirmation of receipt required; encryption optional	No special requirements; encryption optional	No special requirements
By interoffice mail	No external labeling on envelope; normal labeling on document	No special requirements	No special requirements
By voice mail	Confirmation of receipt required (sender); remove message after receipt (recipient)	No special requirements	No special requirements
By electronic messaging (e-mail)	Confirmation of receipt required; encryption optional	No special requirements	No special requirements
By wireless or cellular phone	Do not transmit	No special requirements	No special requirements
By FAX	Attended at receiving FAX	Information *owner* to define requirements	No special requirements

Figure 12.14 Information-handling matrix for electronically transmitted information.

Record	Retain	Record	Retain
Accounts payable schedules	Permanent	General ledgers	Permanent
Accounts receivables schedules	Permanent	Insurance policies	Until expiration
Bank drafts and paid notices	10 years	Internal repair orders (hard copy only)	7 years
Bank statements and reconciliations	10 years	Internal sales journals	Permanent
Bills of lading	7 years	Journal vouchers	Permanent
Cancelled checks	10 years	Miscellaneous schedules	Permanent
Cash disbursements journals	Permanent	New and used vehicle records	7 years
Cash receipts journals	Permanent	New vehicle sales journals	Permanent
Claims register	7 years	Office receipts	7 years
Corporate minutes book	Permanent	Parts, accessories, and service sales journals	Permanent
Correspondence	10 years	Payroll journals	Permanent
Counter tickets	7 years	Prepaid and accrued expense schedule	2 years
CPA audit reports	Permanent	Property tax returns	Permanent
Credit memos	7 years	Purchase journals	Permanent
Customer files	7 years	Purchase orders	7 years
Customer repair orders (both office and hard copy)	7 years	Receiving reports	7 years
Documents pertaining to litigation	Permanent	Repair order check sheet	2 years
Duplicate deposit slips	10 years	Repair orders — internal (office copy only)	2 years
Employee earning and history record	Permanent	Sales invoices	7 years
Employment contracts	Permanent	Salesperson’s commission reports	Permanent
Federal revenue agents’ reports and related papers	Permanent	Social security tax returns	Permanent
Federal tax returns	Permanent	State and local sales tax returns	Permanent
Financial statements	Permanent	State annual reports	Permanent
General journals	Permanent	State franchise tax returns	Permanent
		Sundry invoices	7 years
		Time cards	2 years

Figure 12.15 Sample record retention schedule.

Record	Retain	Record	Retain
		U.S. and State unemployment tax returns	Permanent
		Used and repossessed vehicles journals	Permanent
		Vehicle invoices	7 years

Figure 12.15 (Continued) Sample record retention schedule.

Owners

Minimally, the information owner is responsible for

- Judging the value of the information resource and assigning the proper classification level
- Periodically reviewing the classification level to determine if the status should be changed
- Assessing and defining appropriate controls to assure that information created is properly safeguarded from unauthorized access, modification, disclosure, or destruction
- Communicating access and safeguard requirements to the information custodian and users
- Providing access to those individuals with a demonstrated business need for access
- Assessing the risk of loss of the information and assuring that adequate safeguards are in place to mitigate the risk to information integrity, confidentiality, and availability
- Monitoring safeguard requirements to ensure that information is being adequately protected
- Assuring that a business continuity plan has been implemented and tested to protect information availability

Custodians

At a minimum, the custodian is responsible for

- Providing proper safeguards for processing equipment, information storage, backup, and recovery
- Providing a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information
- Administering access requests to information properly authorized by the owner

User

The user must

- Use the information only for the purpose intended
- Maintain the integrity, confidentiality, and availability of information accessed

Being granted access to information does not imply or confer authority to grant other users access to that information. This is true whether the information is electronically held, printed, hard copy, manually prepared, copied, or transmitted.

Summary

Information classification drives the protection control requirements and this allows information to be protected to a level commensurate to its value to the organization. The cost of overprotection is eliminated and exceptions are minimized. With a policy and methodology in place, specifications are clear and accountability is established.

There are costs associated with implementing a classification system. The most identifiable costs include labeling classified information, implementing and monitoring controls and safeguards, and proper handling of confidential information.

Information, wherever it is handled or stored, needs to be protected from unauthorized access, modification, disclosure, and destruction. All information is not created equal. Consequently, segmentation or classification of information into categories is necessary to help identify a framework for evaluating the information's relative value. By establishing this relative value, it will be possible to establish cost-effective controls that will preserve the information asset for the organization.

The information classification program will require the identification of the record type, the owner, and the classification level. Two-thirds of this information may already be gathered by the record management program. Link these two vital processes together to ensure that employee time is not wasted on redundant activities. By combining these efforts, the organization will have a better overall information security program.

Chapter 13

Threats to Information Security

Justin Peltier

Contents

Editor's Note

Justin became ill in late 2006 and started a 4-year battle spending time with various doctors. In October 2010, he went to sleep one evening and never woke up. His goal was to update this chapter and he was working on doing so at the time of his death. I submit this unedited chapter as a tribute to the man he was and how he will be remembered.

What Is Information Security?

Information security is such a wide-ranging topic that it can be rather difficult to define precisely what it is. So when it came time for me to try to define it for the introduction of this chapter, I was stuck for a long time. Following the recommendation of my wife, I went to the best place to find definitions for anything—the dictionary. I pulled up the *Merriam-Webster* dictionary online and came up with these entries:

Main Entry: in·for·ma·tion
Pronunciation: in-fər-'mā-shən
Function: noun

1: the communication or reception of knowledge or intelligence
2a (1): knowledge obtained from investigation, study, or instruction
(2): INTELLIGENCE, NEWS
(3): FACTS, DATA **b:** the attribute inherent in and communicated by one of two or more alternative sequences or arrangements of something (as nucleotides in DNA or binary digits in a computer program) that produce specific effects **c**(1): a signal or character (as in a communication system or computer) representing data (2): something (as a message, experimental data, or a picture) which justifies change in a construct (as a plan or theory) that represents physical or mental experience or another construct **d:** a quantitative measure of the content of information; specifically: a numerical quantity that measures the uncertainty in the outcome of an experiment to be performed
3: the act of informing against a person
4: a formal accusation of a crime made by a prosecuting officer as distinguished from an indictment presented by a grand jury
—in·for·ma·tion·al/*adjective*
—in·for·ma·tion·al·ly *adverb*

And for security, my result was this:

Main Entry: se·cu·ri·ty
Pronunciation: si-'kyūr-ə-tē
Function: *noun*
Inflected Form(s): *plural*-**ties**

1: the quality or state of being secure: as **a:** freedom from danger: SAFETY **b:** freedom from fear or anxiety **c:** freedom from the prospect of being laid off <job *security*>
2a: something given, deposited, or pledged to make certain the fulfillment of an obligation **b:** SURETY
3: an evidence of debt or of ownership (as a stock certificate or bond)

> **4a:** something that secures: PROTECTION **b**(1): measures taken to guard against espionage or sabotage, crime, attack, or escape (2): an organization or department whose task is security

So even after looking information security up in this dictionary, I still did not have a good way to describe and explain what information security was. Considering that I have worked in information security for almost 9 years now, it was a little unsettling to not be able to define, at the most basic level, what I really did. The biggest difficulty in defining information security is, to me, because defining information security is a little bit like trying to define infinity. It just seems to be far too vast for me to easily comprehend. Currently, information security can cover everything from developing the written policies that an organization will follow to secure its' information to the implementation of a user's access to a new file on the organization's server. With such a wide range of potential elements, it often leaves those in information security feeling as if they are a bit of the "jack-of-all-trades, master of none." To give you a better feeling of the true breadth of information security, we will cover some of the more common aspects of information security in brief. All of the facets that we cover in the next few paragraphs will be discussed in more detail throughout the rest of the book.

The first and probably most important aspect of information security is the security policy. If information security were a person, the security policy would be the central nervous system. Policies become the core of information security, which provides a structure and purpose for all other aspects of information security. To those of you who may be a bit more technical, this may come as a surprise. Even the folks over at Cisco in the documentation for their Cisco PIX firewall product refer to the security policy as the center of security. RFC 2196 "Site Security Handbook" defines a security policy as, "A formal statement of the rules by which people that are given access to an organization's technology and information assets must abide." Because of the central nature of security policies, you cannot discuss information security without mentioning it (Figure 13.1).

Another aspect of information security is organizational security. Organization security takes the written security policy and develops a framework for implementing the policy throughout the organization. This would include tasks such as getting support from senior management, creating an information security awareness program, reporting to an information steering committee, and advising the business units of their roles in the overall security process. The role of information security is still so large that there are many other aspects beyond just the organizational security and security policy.

Yet another aspect of information security is asset classification. Asset classification takes all the resources of an organization and breaks them into groups. This allows for an organization to apply differing levels of security to each of the groups as opposed to security settings to each individual resource. This process can make security administration easier after it has been implemented, but the

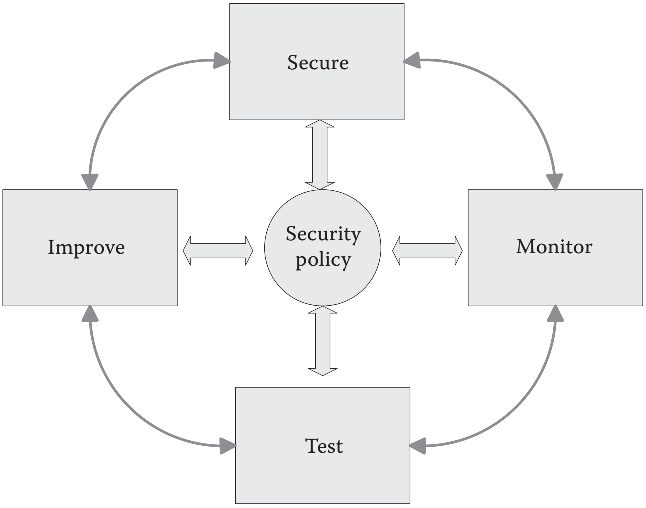


Figure 13.1 Security wheel.

implementation can be rather difficult. However, there is still more to information security.

Another phase of information security is personnel security. This can be both fun and taxing at the same time. Personnel security, like physical security, can often be a responsibility of another person and not the sole responsibility of the information security manager. In small organizations, if the word security is in your job description, you may be responsible for everything. Personnel security deals with the people who will work in your organization. Some of the tasks that are necessary for personnel security are creating job descriptions, performing background checks, helping in the recruitment process, and user training.

As mentioned in the previous paragraph, physical security is a component of information security, which is often the responsibility of a separate person from the other facets of information security. Even if physical security is some other person's responsibility, the information security professional needs to be familiar with how physical security can affect information security as a whole. Often, when an organization is thinking of stopping a break-in, the initial thought is to stop people from coming in over the Internet. When in fact it would be easier to walk into the building and plug into the network jack in the reception area. For years, I've been hearing one story, which I have never been able to verify, that illustrates this example very well.

Supposedly, the CEO of a large company stands up in the general session of a hacker conference and announces, "This is a waste of time. My organization is so secure that if anyone here can break into our computers I'll eat my hat."

Someone in the audience decides that the CEO needs to learn a lesson. The attacker decides to break into the organization, not by using the Internet or their telecommunication connection, but instead decides to take a physical approach to the attack. The attacker walks in the front door of the organization, walks to the second floor server room and proceeds to walk in. Supposedly, the server room was having HVAC problems, so the door had to be propped open to allow the excess heat out. The attacker walks through the rows of devices in the server room and walks up to each of the cabinets and reads the electronically generated label on each device. When he finds the rack with the device marked "Firewall," he realizes he has found what he was looking for. The attacker than proceeds to turn off the firewall, disconnects the cables, and removes the firewall from the rack. The attacker follows this by hoisting the firewall up onto his shoulder and walking into the CEO's office.

When the attacker enters the CEO's office, he has only one thing. He asks, "What kind of sauce would you like with your hat?"

Physical security is much like information security in that in can be immense in its own right. Physical security can encompass everything from closed circuit television to security lighting and fencing to badge access, and heating, ventilation, and air conditioning (HVAC). One area of physical security that often is the responsibility of the information security manager is backup power. The use of uninterruptible power supplies (UPS) are usually recommended even if your organization has other power backup facilities like a diesel generator.

However, there is still more to information security. Another area of information security is communications and operations management. This area can often be overlooked in smaller organizations because it is often mistakenly considered "overhead." Communication and operations management encompasses such tasks as ensuring that no one person in an organization has the ability to commit and cover up a crime, making sure that development systems are kept separate from production systems, and making sure that systems that are being disposed of are being disposed of in a secure manner. Although it is easy to overlook some of these tasks, it can create large security holes in an organization.

Access control is another core component of information security. Following the analogy used previously, if information security is the central nervous system of information security, access control would be the skin. Access control is responsible for allowing only authorized users to have access to your organization's systems and also for limiting what access an authorized user does have. Access control can be implemented in many different parts of information systems. Some common places for access control include

1. Routers
2. Firewalls
3. Desktop operating system
4. File server
5. Applications

Some organizations create something often referred to as a "candyland." A candyland is where the organization has moved the access to just one or two key points usually on the perimeter. This is called a candyland because the organization has a tough crunchy exterior, followed by a soft gooey center. In any organization, you want access control to be in as many locations as your organization's support staff can adequately manage.

In addition to the previously mentioned components of information security, system development and maintenance is another component that needs to be considered. In many of the organizations that I have worked for, we never followed either of these principles. One area of system development and maintenance has been getting a lot of attention lately. Patch management would be a task from the maintenance part of system development and maintenance. This is a task that has many information security professionals referring to themselves as "Patch Managers." With such a large number of software updates coming out so frequently for every device on the network, it can be difficult (if not impossible) for a support staff to keep everything up-to-date. And all it takes is one missed patch on any Internet-facing system to provide attackers a potential entry point into your organization. In addition to keeping systems up-to-date with patches, system development is another area that needs to be security-minded. When a custom application is written for your organization, each component or module of the application needs to be checked for security holes and proper coding practices. This is often done quickly or not at all, and can often lead to large exposure points for the attacker.

In addition to keeping our systems secure from attackers, we also need to keep our systems running in event of a disaster—natural or otherwise. This becomes another facet of information security; often called business continuity planning. Every information security professional should have some idea of business continuity planning. Consider what you would do if the hard drive in your primary computer died. Do you have a plan for restoring all of your critical files?

If you are like me, you probably never plan for a hard drive failure, until after the first one happens. For me, it actually took many failed hard drives before I became more diligent in performing home backups of my critical files. In a large organization, just having an idea of what you would do in the event of a disaster is not enough. A formal plan needs to be written, tested, and revised regularly. This will ensure that, when something much worse than a hard drive dying happens to your organization, everyone will know exactly what to do.

The last aspect of information security that we will discuss here is compliance. Now, you may be thinking compliance is someone else's job. You might be telling the truth, but if we go back to our analogy that if information security is a person, with security policy being the backbone and access control being the skin, then compliance would be the immune system. I know that might be a rather odd comparison, but compliance is a component of information security and I like to think of the compliance folks like a partner to the security folks. Many information security professionals spend some time reviewing and testing information system for completeness and adequacy, and that is compliance.

So maybe you see why information security is so hard to define—it's just huge! With all the phases from policy to telecommunications, there is a lot to it. All of the phases are equally important, because when it comes to threats to an organization, a breakdown in any of the phases of information security can present a gaping hole to the attacker. This is why the information security professional needs to have an understanding of all the aspects of information security.

Common Threats

From the hacker sitting up at all hours of the night finding ways to steal the company's secrets to the dedicated employee who accidentally hits the delete key, there are many foes to information security. Due to the many different types of threats, it is a very difficult to try to establish and maintain information security. Our attacks come from many different sources, so it is much like trying to fight a war on multiple fronts. Our good policies can help fight the internal threats and our firewall and intrusion detection systems can help fight the external threats. However, a failure of one component can lead to an overall failure to keep our information secure. This means that even if we have well secured our information from external threats, our end users can still create information security breaches. Recent statistics show that the majority of successful compromises are still coming from insiders. In fact, the Computer Security Institute (CSI) in San Francisco estimates that between 60% and 80% of network misuse comes from inside the enterprises where the misuse has taken place.

In addition to the multiple sources of information security attacks, there are also many types of information security attacks. A well-known model helps illustrate this point. The information security triad shows the three primary goals of information security. The three components of the triad are integrity, confidentiality, and availability. When these three tenants are put together, our information will be well protected (Figure 13.2).

The first tenant of the information security triad we will discuss is integrity. Integrity is defined by ISO-17799 as, "the action of safeguarding the accuracy and

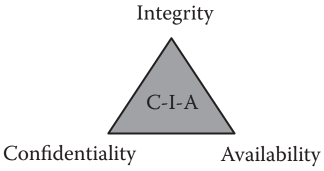


Figure 13.2 CIA triad.

completeness of information and processing methods," which can be interpreted to mean that when a user requests any type of information from the system, the information will be correct. A great example of a lack of information integrity is commonly seen in large home improvement warehouses. One day, I ventured to the local home improvement megamart looking for a hose to fix my sprinkler system. I spent quite some time looking for the hose before I happened upon a salesperson. Once I had the salesperson's attention, I asked about the location and availability of the hoses I was looking for. The salesperson went to his trusty computer terminal and pulled up information about the hose that I needed. The salesperson then let me know that I was in luck and they had 87 of the particular type of hose that I needed in stock. So I inquired to where these hoses could be found in the store and was told that just because the computer listed 87 in the store, it did not mean that there really were any of the hoses. Whereas this example really just ruined my Sunday, the integrity of information can have much more serious implications. Take your credit rating; it is just information that is stored by the credit reporting agencies. If this information is inaccurate, or does not have integrity, it can stop you from getting a new home, car, or job. The integrity of this type of information is incredibly important, but is just as susceptible to integrity errors as any other type of electronic information.

The second tenant of the information security triad we will discuss is confidentiality. Confidentiality is defined by ISO-17799 as "ensuring that information is accessible only to those authorized to have access to it." This can be one of the most difficult tasks to ever undertake. To attain confidentiality, you have to keep secret information secret. It seems easy enough, but remember the discussion on threat sources above? People from both inside and outside of your organization will be threatening to reveal your secret information.

The last tenant of the information security triad is availability. Once again, as defined by ISO-17799, availability is ensuring that authorized users have access to information and associated assets when required. This means that when a user needs a file or system, the file or system is there to be accessed. This seems simple enough, but there are so many factors working against your system's availability. You have hardware failures, natural disasters, malicious users, and outside attackers all fighting to remove the availability from your systems. Some common mechanisms to fight against this downtime are fault-tolerant systems, load balancing, and system failover.

Fault-tolerant systems incorporate technology that allows the system to stay available even when a hardware fault has occurred. One of the most common examples of this is RAID (according to the folks over at linux.org, the acronym RAID means redundant array of inexpensive disks). I have heard much debate as to what those little letters actually stand for, but for our purposes, let's just use that definition. RAID allows the system to maintain data on the system even in the event of a hard drive crash. Some of the simplest mechanisms to accomplish this are through disk mirroring and disk duplexing. With disk mirroring, the system would have two hard drives attached to the same interface or controller. All data would be written to both drives simultaneously. With disk duplexing, the two hard drives are attached to the system through two different controllers. Duplexing allows for one of the controllers to fail with the system losing any availability of the data. However, a RAID configuration can get significantly more complex than disk mirroring or disk duplexing. One of the more common advanced RAID solutions is RAID level 5. With level 5 RAID, data is striped across a series of disks, usually three or more, so that when any one drive is lost, no information is destroyed. The disadvantage with using any of the systems mentioned above is that you lose some of the storage space from the devices. For example, a RAID 5 system with five 80-gigabyte hard drives would only have 320 gigabytes of actual storage. For more information on RAID, refer to the chart in Figure 13.3.

The technologies we have just discussed provide system tolerance, but do not provide improved performance under heavy utilization conditions. To improve system performance with heavy utilization, we need load balancing. Load balancing allows the information requests to be spread across a large number of servers or

RAID level	**Activity**	**Name**
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume is unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data is written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data is created with a hamming code, which identifies any errors. This level specifies the use of up to 39 disks: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it cab be reconstructed from parity drive.	Byte-level parity
4	Same as level 3, except data is striped at the block level instead of the byte level.	Block-level parity
5	Data is written in disk sector units to all drives. Parity is written to all drives also, which ensures that there is not a single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data is simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring

Figure 13.3 RAID chart.

other devices. Usually, a front end component is necessary to direct requests to all of the back end servers. This also provides tolerance because the front end processor can just redirect the requests to the remaining servers or devices.

A technology that would be between load balancing and RAID in terms of the most availability would be system failover. With a failover environment, when the primary processing device has a hardware failure, a secondary device begins processing. This is a common technology to use with firewalls. In most organizations, to avoid having the firewall become the single point of failure on the network, the organization implements two firewalls that communicate with each other. In the event that the primary firewall cannot communicate with the secondary firewall, the secondary firewall takes over and begins processing the data.

As we have discussed previously, the job of the information security manager is difficult. There are many tasks to adequately protect the resources of an organization and one slip along any of them can lead to a systems breach. This is why the task of defending information systems is rather difficult. In the next section, we will look at other ways that your systems can be attacked.

Errors and Omissions

Although errors and omissions do not get the headlines of international hackers and the latest work propagating through the e-mail system, it is still the number one threat to our systems. Because we cannot deny access to all of the user community, it becomes difficult to protect our systems from the people who need to use it day in and day out. Errors and omissions attack the integrity component of the CIA triad that we have discussed previously. To help fight these mistakes, we can use some of the following security concepts.

The first security concept that will help fight error and omissions is "least privilege." If we give our users only the most minimal set of permissions that the user needs to perform their job function, then we reduce the amount of information that can be accidentally contaminated. Using least privilege can create additional overhead on the support staff members that are tasked with applying access controls to our user community. However, it will be worth the additional changes to keep the integrity of our information systems.

Another principle that can help is performing adequate and frequent backups of the information on the systems. When the user causes loss of integrity of the information resident on the system, it may be easier to restore the information from a tape backup made the night before. Tape backups are one of the essential tools of the information security manager and can often be the only the only recourse against a successful attack.

Fraud and Theft

If your end users are not accidentally destroying data, but are maliciously destroying the information, then you may have a completely different type of attack. For most employees, it is difficult to imagine a fellow employee coming into work every day under a ruse, but it does happen. As we stated before, employees are responsible for more successful intrusions than outsiders. It becomes very difficult to find the source of internal attacks without alerting the attacker that you suspect them of the wrongdoing. The best line of defense against fraud and theft by your internal employees are well-defined policies. These policies can make it easier for the information security manager to collect data on the suspected wrongdoer to prove what bad acts have been performed by the employee.

If you have well-defined policies in your organization, the information security manager can use forensic techniques to gather evidence that will help provide proof of who performed the attack. Although the entire breadth of forensics is beyond the scope of this book, we will spend a little time here to talk about forensics from a high level.

Computer forensics allows a trained person to recover evidence from computer systems. The first rule of computer forensics is "do no harm." This means that if you are not sure what to do—do not do anything to the system. The first goal of computer forensics is to leave the system in as pristine condition as possible. This may run counterintuitive to the technology professional, whose instincts want to look at the system to determine exactly what is going on and how it happened. Every time the technical professional moves the mouse or touches the keyboard to enter a command, the system is changing. This makes the evidence gathered from the system more suspect. After all, how would we determine what was done by the suspected employee and what was done by the professional investigating the activity?

There are many places in which evidence of the activity may have been left behind. Firewalls, server logs, and the client workstation are all places that need to be investigated to determine if any evidence remains. When it comes to the client workstation, the first step in computer forensics is very nontechnical. In this first step, the security or support staff should be contacted to see what details they know about the system. One of the biggest potential problems would be if the client was using a hard drive encryption utility. The reason for this is that the second step is to "pull the-plug." If you pull the plug on a system that has an encrypted hard drive, you may never be able to determine what information was on that system. We will talk more about encryption in a later chapter of this book.

Assuming that you are able to confirm that there is no hard drive encryption on the suspect system, the next step is—as mentioned above—to pull the plug. Now if the system is a laptop, pulling the plug will not shut the system down, it will just run off of the battery. In the case of the laptop, you need to pull the plug and remove the battery as well. In any case, once the system is powered off, the hard drive in the system should be turned over to a qualified professional. Please note that there are actually many more steps in the forensic process that are just beyond on the scope of this book.

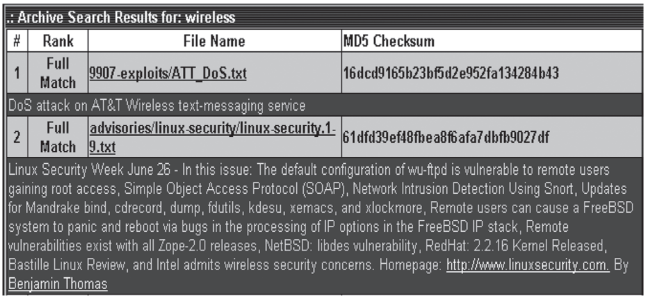
Once the qualified professional has the suspect system, or at least the hard drive, the professional will then make a bit stream backup of the hard drive. A bit stream backup is different from a regular tape backup in that it makes an exact copy of the hard drive. A bit stream backup does not just copy the files and the file system, it copies everything. The blank space, the slack space, file fragments, and everything else gets copied to a second hard drive. The reason for this is that all the data recovery processes will be done on the second hard drive, leaving the original hard drive in its pristine state and unmodified. All data recovery processes that will be performed on the system will be done on the backup copy of the hard drive.

Once the copy is made, a comparison of the hard drives will be done using an integrity technology called an MD5 hash. The definition for an MD5 hash as taken from the MD5 web page is as follows: "(The MD5 algorithm) takes as input a message of arbitrary length and produces as output a 128-bit 'fingerprint' or 'message digest' of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.

In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods."

Once the MD5 hashes are made from each hard drive, the corresponding values can then be compared. If these values are the same, then the two drives are identical. If the MD5 values are different, then the bit stream backup failed and the drives are different. MD5 hashes are quite commonly used to verify the integrity of a file. The values can be used to ensure that a file was not modified during download and can also be used as a component of a digital signature (Figure 13.4).

After the hard drives have been compared and found to be identical, the forensic professional would then begin looking at the hard drive for evidence that the attack was launched from that machine. The forensics professional will try to recover deleted files, will look for file fragments in slack space, and will also look through the data files on the suspect system to see if any evidence is present. If any evidence is found on the system, the forensic professional will document the evidence and turn it into a final written report.



.: Archive Search Results for: wireless

#	Rank	File Name	MD5 Checksum
1	Full Match	9907-exploits/ATT_DoS.txt	16dcd9165b23bf5d2e952fa134284b43
DoS attack on AT&T Wireless text-messaging service			
2	Full Match	advisories/linux-security/linux-security.1-9.txt	61dfd39ef48fbea8f6afa7dbfb9027df
Linux Security Week June 26 - In this issue: The default configuration of wu-ftpd is vulnerable to remote users gaining root access, Simple Object Access Protocol (SOAP), Network Intrusion Detection Using Snort, Updates for Mandrake bind, cdrecord, dump, fdutils, kdesu, xemacs, and xlockmore, Remote users can cause a FreeBSD system to panic and reboot via bugs in the processing of IP options in the FreeBSD IP stack, Remote vulnerabilities exist with all Zope-2.0 releases, NetBSD: libdes vulnerability, RedHat: 2.2.16 Kernel Released, Bastille Linux Review, and Intel admits wireless security concerns. Homepage: http://www.linuxsecurity.com. By Benjamin Thomas			

Figure 13.4 Web site with MD5 values.

Because we have been looking at the damage that internal employees can do against our information systems, let us look at another community that can also cause destruction to our data—the outsiders.

Malicious Hackers

There are several groups of Internet users out there that will attack information systems. The three primary groups are hackers, crackers, and phreaks. Although common nomenclature is to call all three of the groups "hackers," there are some differences between the groups. A hacker is a user who penetrates a system just to look around and see what is possible. The etiquette of the hacker is that after they have penetrated the system, they will notify the system administrator to let the administrator know that the system has vulnerability. It is often said that a hacker just wants security to be improved on all Internet systems. The next group, the crackers, is the group to really fear. A cracker has no etiquette on breaking into a system. A cracker will damage or destroy data if they are able to penetrate a system. The goal of the cracker is to cause as much damage as possible to all systems on the Internet. The last group, phreaks, tries to break into your organization's phone system. The phreaks can then use the free phone access to disguise the phone number that they are calling from, and also stick your organization with the bill for long-distance phone charges.

The way that a hacker will attack a system can vary tremendously. Each attacker has their own bag of tricks that they can use to break into a system. There are several books currently available on just the subject of hacking, but we will cover the basic hacker methodology briefly here.

The basic hacker methodology has five main components—reconnaissance, scanning, gaining access, maintaining access, and covering tracks. It might seem odd to think of a methodology for hackers, but as with anything else, time matters. So to maximize time, most hackers follow a similar methodology.

The first phase in the methodology is the reconnaissance phase. In this the phase, the attacker tries to gain as much information about the target network as possible. There are two primary ways an attacker can do this—active and passive. Most attackers would generally begin with passive attacks. These passive attacks can often generate a lot of good information about the network or organization the hacker wants to attack. The hacker would often begin by reading through the web site of the organization to see if any information can be gained. The attacker would look for contact information for key employees (this can be used for social engineering), information on the types of technology used at the organization, and any other nugget of information that could be used in an attack. After the attacker has gone through the web site, he would probably move to Internet search engines to find more information about the network he or she wishes to attack. The attacker would be looking for bad newsgroup postings, posts at sites for people who are upset with the company, and any other details that could help in the attack. The attacker would then look for information in the DNS servers for the attack organization. This would provide a list of servers and corresponding IP addresses. Once this is done, the hacker would move on to active attacking.

To perform an active reconnaissance attack, a hacker would perform ping sweeps, SNMP network scans, banner grabbing, and other similar attacks. The attacks would help the attacker weed out the number of dead IP addresses and find the live hosts to move on to the next phase—scanning.

An attacker would begin scanning—looking for holes to compromise to gain access to the network. The attacker would scan all servers that are available on the Internet, looking for known vulnerabilities. These vulnerabilities could be in a poorly written web-enabled application or from applications that have known security vulnerabilities in them. The attacker would also look at the organization's firewall and routers to see if vulnerabilities exist there as well. Once an attacker has compiled a list of vulnerabilities, than he or she would move on to the next stage—gaining access.

There are many ways for an attacker to gain access to the target network. Some of the more common entry points into the network are through the target server's OS, through an application that was developed in-house, as well as through an application with known vulnerabilities, through network devices that can be seen from the Internet and, if all else fails, the attacker can perform a denial-of-service (DoS) attack. Once the attacker has access, all the attacker wants to do is make sure that he or she can keep it.

To maintain access, an attacker would commonly upload custom application onto the compromised server. These applications would then be backdoors into the target organization, and would allow the attacker to come and go at will. Besides just uploading new programs, an attacker can alter existing programs on the system. The advantage to doing this is that a well-informed administrator might know the files on his or her system and might recognize if new files were installed on the servers. By modifying already existing files, the system would appear to be unmodified at first glance. One common way of doing this is with a group of files called a rootkit. A rootkit allows an attacker to replace normal system files with files of the same name that also have Trojan horse functionality. The new system files would allow the attacker in just as if he or she added additional files to the target server. An attacker may not need a long period of access to the system and might just wish to download the existing programs or data off of the target server. Once an attacker has put the mechanism for getting back into the server, the last step in the hacker methodology is to cover the tracks.

To cover the tracks, an attacker would go through the system audit log files and remove any trace of the attacker on the system. This would hide the attacker's access from the system administrator and would also leave less evidence behind in case the system administrator wishes to have a forensic examination performed on the compromised host. The level of skill of an attacker is often apparent in this phase. A crude attacker may delete then entire log file, making it easy for the system administrator to determine that someone has been in the system, but a more skillful attacker may just modify his or her log entries to show that the traffic was originating from a different IP address.

Malicious Code

Although malicious users can attack your system, programs released by the same group of people will often be more successful in reaching the protected parts of your organization. Malicious code is defined as any code that is designed to make a system perform any operation with the knowledge of the system owner. One of the fastest ways to introduce malicious code into a target organization's protected network is by sending the malicious code via e-mail.

There are many different types of malicious code. In this chapter, we will look at a few of the more common ones including viruses, worms, Trojan horses, and logic bombs. The most commonly thought of type of malicious code is the virus. A virus is a code fragment, or a piece of code, that can be injected into target files. A virus then waits, usually until the file is opened or accessed, to spread to another file where the malicious code is then injected into that file. With a virus-infected system, you can often find more than 30,000 infected files. There are many different types of viruses out there. There are viruses that attack the boot sector of the hard drive, there are file system infectors, there are macro viruses that use the Office scripting functionality, and there are viruses for all major operating systems.

Another type of malicious code is the worm. A worm is typically a complete file that infects one place on a given system and then tries to replicate to other vulnerable systems on the network or Internet. A number of highly publicized attacks have, lately, been worms. Nimda is one example of a recent highly publicized attack that was a worm.

Trojan horses are a different type of malicious code and can be quite deceiving to the end user. A Trojan horse appears to have a legitimate function on the surface, but has malicious code underneath. There are a number of freeware programs on the Internet that allow an attacker to insert any malicious code that the attacker wants to send into most of the common executables. The only way to help stop a Trojan horse is to educate the end user to not open file attachments unless they know exactly what the attachment will do.

The last type of malicious code that we will look at is the logic bomb. The logic bomb is a generic term for any type of malicious code that is waiting for a trigger event to release its payload. This means that the code could be waiting for a time, such as 1 month, before it executes. A well-known example of a logic bomb was the Michelangelo attack. This logic bomb was waiting for Michelangelo's birthday before it would trigger its malicious code.

Denial-of-Service Attacks

As an attacker, if you cannot get access to the target network, often the next best thing that you can do is make sure that no one gets access to the network. Enter the DoS attack. The DoS attack is designed to either overwhelm the target server's hardware resources or to overwhelm the target network's telecommunication lines. For years, there were a number of common "one-to-one" DoS attacks. In these attacks, the hacker would launch an attack from his or her system against the target server or network. Syn floods, Fin floods, Smurfs, and Fraggles are all examples of these one-to-one attacks. Although all these attacks could still be successful on some target networks today, most organizations have implemented technologies to stop these attacks from causing service disruptions in their organizations.

In February of 2000, a DoS attack hit the next level. In that month, a number of high-profile targets were taken off-line by the next generation of DoS attacks—the distributed DoS (DDoS). These DDoS attacks were no longer the familiar one-to-one attacks of the past. These attacks used zombie hosts to create a many-to-one attack. These zombie hosts were devices that were compromised and had code uploaded onto them that would allow for a master machine to contact them, and have them all release the DoS attack at the same time. There were tens of thousands of zombie hosts available and the attacker could use a number of common tools to launch the attack from. Some of the common tools were Trinoo, TFN2K, and stacheldraht. These tools were pretty straightforward to use and allowed for an attacker to release a devastating attack against the target.

The new DDoS attacks are very difficult to defend against. Most of the tools denied service not by overwhelming the processing server, but by flooding the telecommunications lines from the Internet service provider (ISP). Most organizations are still vulnerable to this sort of attack. The mechanism that has curtailed most of the DDoS attacks currently is by trying to minimize the number of zombie-infected hosts available. As soon as a new, and better infection mechanism surfaces, another round of DDoS attacks are sure to spring up.

Social Engineering

Social engineering is the name given to a category of security attacks in which someone manipulates others into revealing information that can be used to steal data, access to systems, access to cellular phones, money, or even your own identity. Such attacks can be very simple or very complex. Gaining access to information over the phone or through web sites that you visit has added a new dimension to the role of the social engineer.

During this session, we will examine ways in which people, government agencies, military organizations, and companies have been duped into giving information that has opened them to attack. We will also look at the low-tech as well as the newer forms of electronic theft.

Social engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider, based on the building of an inappropriate trust relationship with insiders. Please note that the term "outsider" does not refer only to nonemployees. An outsider can be an employee that is attempting to circumvent established policies and standards.

The goal of social engineering is to trick someone into providing valuable information or access to that information or resource. The social engineering exploiter preys on qualities of human nature, such as

- The desire to be helpful. We have trained our employees well. Make sure the customer is satisfied. The best way to a good appraisal is to have good responses from those needing assistance. Most of our employees want to be helpful and this can lead to giving away too much information.
- A tendency to trust people. Human nature is to actually trust others until they prove that they are not trustworthy. If someone tells us that they are a certain person, we usually accept that statement. We must train our employees to seek independent proof.
- The fear of getting into trouble. Too many of us have seen negative reaction by superiors because verification of identity took too long or that some official was offended. Management must support all employees that are doing their assignment and protecting the information resources of the enterprise.
- The willingness to cut corners. Sometimes, we get lazy. We post passwords on the screen or leave important material lying out.

What scares most companies about social engineers is that the sign of a truly successful social engineer is that they receive what they are looking for without raising any suspicion. It is the bad social engineers that we know about, not the good ones.

According to the *Jargon Dictionary*, "wetware" is the human being attached to a computer system. People are usually the weakest link in the security chain. In the 1970s, we were told that if we installed access control packages, then we would have security. In the 1980s, we were encouraged to install effective antivirus software to ensure that our systems and networks were secure. In the 1990s, we were told that firewalls would lead us to security. Now in the twenty-first century, it is intrusion detection systems or public key infrastructure that will lead us to information security. In each and every iteration, security has eluded us because the silicon-based products have to interface with carbon-based units. It is the human factor that will continue to appear in our discussion on social engineering.

A skilled social engineer will often try to exploit this weakness before spending time and effort on other methods to crack passwords or gain access to systems. Why go through all the trouble of installing a sniffer on a network, when a simple phone call to an employee may gain the needed user ID and password?

Social engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone. A successful defense will require an effective information security architecture; starting with policies and standards and following through with a vulnerability assessment process.

Common Types of Social Engineering

Although the greatest area for success is human-based interaction by the social engineer, there are also some computer-based methods that attempt to retrieve the desired information by using software programs to either gather information or to deny service to a system. One of the most ingenious methods was first introduced to the Internet in February 1993. The user attempting to log-on to the system was met with the normal prompt and, after entering the correct user ID and password, had the system begin the prompt all over again. What had happened was that a social engineer managed to get a program installed in front of the normal sign-on routine, gathered the information, and then passed the prompt to the real sign-on process. According to published articles at the time, more than 95% of regular users had their access codes compromised.

Today, a common ploy we see in web sites is to offer something free or a chance to win something on that web site to gain important information. At a Michigan firm in 1998, the network administrator installed a 401K information web site that required employees to register with the site to obtain information on their 401K program. After giving such information as account ID, password, social security number, and home address, the web site returned a message that indicated it was still under construction. Within a week, nearly every employee with a 401K, including senior management, had attempted to register to that web site.

Other forms of social engineering have been classified into various groups. The first two are *impersonation* and *important user*. These two are often used in combination with one another. In the 1991 book *Cyberpunk* by Katie Hafner and John Markoff, the actions of one Susan Hadley (aka Susan Thunder) are described. Using an easily accessible military computer directory, she was able to obtain the name of the individual in charge. She used her basic knowledge of military systems and terminology as she called a military base to find out who the commanding officer was of the secret compartmentalized information facility. She sweet-talked her way into obtaining the name of the Major's secretary and then hung up.

Using this information, she changed tactics. She switched from being nonchalant to authoritative. Her boss, the Major, was having problems accessing the system and she wanted to know why. Using threats, she obtained access and, according to her, was in the system within 20 minutes.

Pretending to be someone you are not, or schmoozing your way to the information you need, these are typical examples of how social engineers work to obtain the information they need. They will often contact the help desk and drop the names of other employees. Once they have what they need to gain further access, they will attack a more vulnerable person; one that has information, but not necessarily the clout, to challenge anyone "of authority."

Perhaps two of the oldest forms of social engineering are *dumpster diving* and *shoulder surfing*. The dumpster diver is willing to get dirty to get the information they need. Too often, companies throw out important information. Sensitive information, manuals, and phone books should be shredded before disposal.

The shoulder surfer will look over someone's shoulder to gain passwords or PIN numbers. A few years ago, one of the news magazine shows did a session on phone card fraud. During one sequence, the reporter was given a new phone calling card and was told to use it at Grand Central Station in New York. While she made the call, the undercover police counted at least five people surfing her PIN number. One even turned to the cameraman to make sure he got the number, too.

The final two types of human-based social engineering are *third-party authorization* and *tech support*. The typical third-party authorization is when the social engineer drops the name of a higher-up who has the authority to grant access. It is usually something like "Ms. Shooter says it's OK" or "Before she went on vacation, Ms. Shooter said I should call you to get this information." The social engineer may well have called the authorities office to find out if they were out. Remember, most social engineers are internal.

The tech support method is where the social engineer pretends to be someone from an infrastructure group and wants a user to access the system while they scope out the connection. They will normally ask for the user's account ID and password so that they can see it cross the network. In a recent vulnerability assessment of a large Texas-based insurance provider, 12 employees were called by "network administration" (actually, the security staff posing as network administration). The employees were told that the network was having connection problems and that they had installed a scope on the fiber connections and asked the employee to log-on to the system. They requested the account ID and password to use as verification that data was being properly sent. Three employees did not answer the phone call. Eight out of the other nine gave the information requested. One employee couldn't give out his password because he couldn't find the Post-it note he had written it on.

Some potential security breaches are so mundane that they hardly seem to be of concern. With all the fires that we have to fight each day and the deadlines we have to meet, sometimes the most obvious is often overlooked.

Passwords—the number one access point for social engineers is the good old-fashioned password. After all of the awareness programs and reminder cards, we still find that employee-generated passwords are too short or too easy to guess. System-generated passwords are too long and employees have to write them down to remember them. Even today, some systems do not require passwords to be changed. We find this most often in e-mail systems and Internet accounts. We recommend an assessment of the password length and interval for change standards. See if they still meet the current needs of the user community.

Modems—every company has more modems than they know about. Employees and contractors will add a modem to a system and then install products like *pcAnywhere* or *Carbon Copy* to improve their remote access time. We recommend that war dialers be used at least twice a year to check on modems.

Help Desk—we've discussed this before. Put in place processes that can assist the help desk employee in verifying who is on the other end of the phone call.

Web sites—two problems here, the dummy site that gathers information and the legal site that gives away too much information. Many hackers use the information that they gather from the enterprise web site to launch attacks on the network. Make certain that the information available will not compromise the information resources of the enterprise.

A social engineer may simply walk in and behave like an employee. Our employees have not been trained to challenge strangers. Or if they have been trained, there has not been enough reinforcement of the challenge process. Require that all personnel onsite wear appropriate identification. Some organizations require only visitors to wear badges. Therefore, to become an employee, a visitor must simply remove the badge. Sell the principle that employee identification is not just a security measure, but it is a process to protect the employees in the workplace. By ensuring that only authorized personnel are permitted access, the employees will have a safe work environment.

Because there is neither hardware nor software available to protect an enterprise against social engineering, it is essential that good practices be implemented. Some of those practices might include the following:

- Require anyone there to perform service to show proper identification
- Establish a standard that passwords are never to be spoken over the phone
- Implement a standard that forbids passwords from being left laying about
- Implement caller ID technology for the help desk and other support functions
- Invest in shredders and have one on every floor

Policies, procedures, and standards are an important part of an overall antisocial engineering campaign. To be effective, a policy should include the following:

- It should not contain standards or directives that may not be attainable
- They should stress what can be done and stay away from what is not allowed as much as possible
- They should be brief and concise
- The need to be reviewed on a regular basis and kept current
- They should be easily attainable by the employees and available via the company Intranet

To be effective, policies, procedures, and standards must be taught and reinforced to the employees. This process must be ongoing and must not exceed

6 months between reinforcement times. It is not enough to just publish policies and expect them to read, understand, and implement what is required. They need to be taught to emphasize what is important and how it will help them do their job. This training should begin at new employee orientation and continue through employment. When a person becomes an ex-employee, a final reinforcement should be done during the exit interview process.

Another method to keep employees informed and educated is to have a web page dedicated to security. It should be updated regularly and should contain new social engineering ploys. It could contain a "security tip of the day" and remind employees to look for typical social engineering signs. These signs might include such behaviors as

- Refusal to give contact information
- Rushing the process
- Name-dropping
- Intimidation
- Small mistakes
- Requesting forbidden information or accesses

As part of this training or education process, reinforce a good catch. When an employee does the right thing, make sure they receive proper recognition. Train the employees on who to call if they suspect they are being social-engineered.

Apply technology where you can. Consider implementing trace calls if possible or at least caller ID where available. Control overseas long-distance services to most phones. Ensure that physical security for the building and sensitive areas are effective.

A social engineer with enough time, patience, and resolve will eventually exploit some weakness in the control environment of an enterprise. Employee awareness and acceptance of safeguard measures will become our first line of defense in this battle against the attackers. The best defense against social engineering requires that employees be tested and that the bar of acceptance be raised regularly.

Summary

Security professionals can begin this process by making available to all personnel a broad range of supporting documentation. Many employees respond positively to anecdotes relating to social engineering attacks and hoaxes. Keep the message fresh and accurate.

Include details about the consequences of successful attacks. Do not discuss these attacks in terms of how security was circumvented, but on their effect on the business or mission of the enterprise. These attacks can lead to a loss of customer confidence, market share, and jobs.

Employees at all levels of the enterprise need to understand and believe that they are important to the overall protection strategy. Without all employees being part of the team, the enterprise, its assets, and its employees will be open to attack from external and internal social engineers. With training and support, we can lessen the effect of these kinds of attacks.

Chapter 14

Information Security Policies: A Practitioner's View

Charles Johnson

Contents

The writing of information security policies is what makes most information security practitioners leap to their feet in the morning to do—NOT! Many practitioners struggle with this area of our chosen profession. But have no fear, there are those lurking in the shadows that do enjoy writing. I may not be the best one at writing policies, but I have been asked repeatedly to write policies for companies and corporations for more than 25 years.

> The time to begin writing an article is when you have finished it to your satisfaction. By that time you begin to clearly and logically perceive what it is you really want to say.
>
> **—Mark Twain**

I learned early in my information security career that engineers or technologists want to be engineers or technologists and play with hardware, cables, cards, etc. They do not want to write or document anything—with one exception—give them a white board and a marker, and they will draw you a diagram that will provide clarity to the meaning of life. Well, maybe not that far, but you get the gist of what I am saying. They are visual learners and communicators of information. And, in my opinion, we all need some form of both visual and verbal communication to grasp something.

I was very fortunate to learn this early and I also learned that if I sat next to an engineer or technologist, they would be all too kind to share with me what they were doing, and how all the pieces went together. And I was astute enough to write all that down, and confirm any areas that were vague or missing some level of clarity. Then, like a thief in the in the night, I would scamper off and prepare a more formal typewritten form and ask them to confirm or deny what was said. In the end, we would both agree that we have a working document and it would then be archived or shared as deemed appropriate.

Definitions

First, let us begin with providing some definitions of Policies, policies, standards, and procedures.

Many of my friends in the information security space have the same opinion as I do about Policies (with a capital "P"). Information security policies are "the bottom line," they set the boundaries of acceptability across the organization. They are the rules or high-level statements for protecting people or systems in the organization. They are intended to be read by a person, such as an employee, contractor, consultant, and temporary personnel. Anyone doing work for the company or on behalf of the company should be familiar with the companies' policies.

The little "p" version of policies is, for the most part, referencing the specific attributes or controls that are defined in a system, an appliance, security application, or even some business applications. These configurable settings or attributes are often referred to as "policies" (with a small "p").

As for the term "standard," it is sometimes used when talking about information security policies, standards, and procedures. Standards are a consistent set of low-level attributes or controls that are applied and replicated consistently across hardware platforms or embedded in software during development, as well as in the configuration of security appliances that will enforce a given policy.

“Procedures” are the how-to, step-by-step processes of actually implementing the standards and satisfying the company policies.

Gather Requirements

Now that we have those definitions out in the open, it is worth pointing out that there may be some areas within your company that are more security-sensitive than others. In these areas, more stringent security measures may be appropriate. Thus, they not only satisfy the Company Information Security Policy but they also exceed the specifications defined in the specific security standard that the company has published. This is permissible and should be communicated as well because it further supports a “defense-in-depth” security methodology that many larger organizations prescribe to. The concept of defense-in-depth is to make use of multiple security layers of defense to protect the information assets of the enterprise.

Before beginning to write information security policies, we know our information security requirements can be obtained from a variety of sources (e.g., legislation, policies, directives, regulations, standards, and organizational, mission/business/operational requirements). Organization-level security requirements are documented in the Information Security Program Plan or an equivalent document.

Conduct Risk Assessment

Before designing and enacting policy, and before selecting and implementing technical security measures, you should always ensure you have a reasonable picture of the risks that your sensitive resources face. This is accomplished through a well-developed and implemented information risk management program. The risk management program can be an excellent source of content for building your information security policies, and it will aid you in prioritizing your work in both developing the policies and in what to focus on first in remediation efforts, etc. We discussed risk management earlier in this book (Chapter 4).

The most simplified form a risk assessment can take while still yielding the necessary information to prioritize and plan security policy development involves the measure of two factors in assessing a given risk. These two factors are, first, determining the probability of the threat being realized, and second, determining the effect if the threat materializes. Each threat should be assigned a value for each of these two factors, and these two factors should then be compared to produce a general risk level that can be used to prioritize risks. From this point, you are now aware of what you need to work on—setting your priorities along with what security policies might be needed. Document all your findings in a manner that works for you. I personally like spreadsheets that I create into crosswalks or matrices. This proves to be very beneficial in presenting to senior leadership because you can convert the data into charts or diagrams very easily, whereas in a matrix format, there is a level of simplified understanding.

Use ISO 27002 as Framework

Now you will want to begin identifying a framework, methodology, or foundation for your organization's information security policies. An approach, methodology, or foundation that I believe is critical to long-term growth and forward thinking toward compliance to Federal, State, legal, or contractual obligations can be found in International Standards Organization (ISO). In my review of many regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), Graham Leach Blyley Act (GLBA), Federal Information Security Management Act (FISMA), etc., a recurring theme is at the root of all these works. That theme is what is now called International Standards Organization's (ISO's) 27000 series and can be found in nearly all regulatory or industry-specific requirements. Many of the more recent state-level legislations have taken on the flavor of ISO. So, it makes sense to me to go to the source and build your policy framework from this standard.

My first step was to create a crosswalk spreadsheet closely examining the categories in ISO for use in my Enterprise Information Security Policy Framework. As mentioned previously, let's begin with a risk management program; specifically, risk assessment. I gathered the information I needed from a risk assessment of my employer's environment, which enabled me to determine where there were strengths and weaknesses. It would also allow me to ensure that the policies developed are in line with what the organization needs.

Policy Format Issues

I shared a number of written policies covering a wide variety of topics with the author. These will allow you to "jump start" your information security policy program much quicker. Of course, you will want to perform your own assessment of what you need in the form of policies because not all may apply within your organization. Another point I feel I need to make here is that you should understand and have a solid working knowledge of your organization's culture. Although I have tried to write these shared polices in a generic manner, we are shaped by our experiences and it is possible that the style of my policies does not fit within your organization's culture. Once you have compared your organization's culture, feel free to use the content within these policies as needed.

Formatting is another area of concern. The format of my policies is a format that my organization did not use at the time. However, because information security was gaining significant attention, I was given some liberty in creating my "own" look and feel of information security policies, standards, or procedures. My MS

Word document templates were created in red, green and blue to represent policies, standards, and procedures, respectively. Therefore, not only is the reader getting the information they need in written form but it was also re-emphasized through the color associated with each one.

To summarize where we are at this point, we have identified the following approach to developing your information security policy program:

1. Gather security requirements—regulatory, contractual, and legal
2. Conduct a risk assessment—identify data and assess risk probability
3. Use ISO 27002 framework—capture in a crosswalk as your model

This is the bedrock of developing your information security policy development program. Over the course of time, you will modify the information contained in your model or methodology as changes occur within the organization and with the inevitable changes in regulatory, contractual, and legal requirements.

In developing the information security program for my organization as changes occurred in the organization, I would enhance or modify some of my parameters. This kept my program evergreen and current with changes in all areas. Our IT audit department found this to be tremendously helpful when conducting periodic audits. Visualize, if you will, my crosswalk was a spreadsheet that listed the regulatory, contractual, or legal requirements along with the specific international standard(s) it supported; in my case, these were row headings and my policies were identified in the column headings. Where they intersected was a connection point where I designed links to the actual controls that were implemented to meet the requirements. Again, our IT audit team was ecstatic as it provided an efficient way for them to audit. Additionally, the benefits of this approach provided our IT security department with real-time immediate information to support any request, internally or externally.

Categorize Your Audience

Now that we have captured the information that we need to address all the concerns of the organization, we need to think about our audience. Your audience of course is all the employees in the company, but this can be divided into groups.

1. Management group
2. Technical group
3. End user group

The core group that everyone would fit in is the end user group. In some instances, you will have employees in two groups and some in all three groups.

Now that we have defined our employee groups, let's briefly cover the fundamental reasons for policies in the first place as this will aid us in determining content for each employee group. The security policy should

1. Aid in tracking compliance with regulations and legislation
2. Establish a basis to minimize risk
3. Establish the company boundaries on security
4. Set the rules for expected behavior by users, system administrators, security personnel, and management
5. Protect people and information
6. Define and authorize security personnel to monitor, probe, and investigate
7. Define and authorize the consequences of a violation

Select Topics

Now, most seasoned security practitioners know from experience that well-defined policies will aid in turning employees into active participants in securing the organization's information assets. Instead of having a team of five security professionals in an organization of 31,000 employees, we turned that around to make information security everyone's responsibility and, thus, enlisted their aid and the help of many who, over time, turned a fledgling information security group into a powerful resource that management called upon extensively.

This approach set into motion many initiatives that otherwise would not have been realized and may have caused extreme embarrassment to the organization as a whole should a breach have occurred.

Our own employees can be our greatest asset because they know the data, they know its value, and they know its weaknesses within the system. So, the employees can be an excellent source of "inside" information that will help you in designing the proper controls for the information you are working with. Of course, the opposite side of the coin is also true. The dishonest employee can be our worst enemy, as they can exploit the vulnerabilities and steal the information for mostly personal and financial gain.

So, let's get back to our different audiences and the types of policies for each one. In my design of the information security policy, the policy should be read by all employees, contractors, consultants, or contingent workers. This policy gives the reader the necessary information on what is of major importance to the management of the company. It provides clear guidance on what is acceptable use of the companies' resources and that there is no expectation of privacy. Here is a brief list of some of the items, which one may find in a policy at this level, that are applicable to all employees.

1. Define the responsibilities of the Security Department
2. E-mail and Internet usage
3. Appropriate use and ethical conduct
4. User identification/administration
5. Managing user accounts

There are many more topics that can be added to this list. With a bit of research, you too can find lists on the web to help stimulate your thinking processes and drive forth what is needed for you and your organization.

So, let's quickly review what we have covered on developing your information security policy program:

1. Gather security requirements—regulatory, contractual, and legal
2. Conduct a risk assessment—identify data and assess risk probability
3. Use ISO 27002 framework—capture in a crosswalk as your model
4. Categorize your audience—select the material most appropriate for the reader
5. Select topics for your policies—cover all aspects of the enterprise

Summary

I believe that once you have built out this information—you should document it. This becomes your foundational document that, if needed, can be referenced upon or shared if audited. You will not be able to write and gain approval for all your policies at one time. Some policy creation will take weeks or months to write and review, and you may have to seek additional information. But this foundational document becomes your pathway to progress. This goes a long way from an auditor's perspective.

There is a wealth of security practitioners who have written many books, and who have greater knowledge than I about how to write policies. Seek out these writers and authors—gather your information and begin developing your plan. In the end, it is about getting started and staying with it for the benefit of your company.

Reference

Thomas R. Peltier, *Information Security Risk Analysis*. 3rd ed. New York: Auerbach Publications, 2010.

Glossary

802.11: Family of IEEE standards for wireless LANS first introduced in 1997. The first standard to be implemented, 802.11b, specifies from 1 to 11 Mbps in the unlicensed band using direct sequence spread spectrum technology. The Wireless Ethernet Compatibility Association (WECA) brands it as Wireless Fidelity (Wi-Fi).

802.1X: An IEEE standard for port-based layer two authentications in 802 standard networks. Wireless LANS often use 802.1X for the authentication of a user before the user has the ability to access the network.

A

Abend: Acronym for abnormal end of a task. It generally means a software crash

Acceptable Use Policy: A policy that a user must agree to follow to gain access to a network or to the Internet

Access Controls: The management of permission for logging on to a computer or network

Access Path: The logical route that an end user takes to access computerized information. Typically, it includes a route through the operating system, telecommunications software, selected application software, and the access control system

Access Rights: Also called permissions or privileges, these are the rights granted to users by the administrator or supervisor. These permissions can be read, write, execute, create, delete, etc.

Accountability: The ability to map a given activity or event back to the responsible party

Administrative Controls: The actions/controls dealing with operational effectiveness, efficiency, and adherence to regulations and management policies

Algorithm: A well-defined set of instructions for manipulating given variables

Anonymous File Transfer Protocol: A method for downloading public files using the file transfer protocol (FTP). Anonymous FTP is called anonymous because users do not provide credentials before accessing files from a particular server. In general, users enter the word anonymous when the host prompts for a username; anything can be entered for the password, such as the user's e-mail address or simply the word guest. In many cases, an anonymous FTP site will not even prompt for a name and password

Antivirus Software: Applications that detect, prevent, and possibly remove all known viruses from files located in a microcomputer hard drive

Application Controls: The transaction and data relating to each computer-based application system. Therefore, they are specific to each such application control, which may be manual or programmed, are to endure the completeness and accuracy of the records and the validity of the entries made therein resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch controls, and encryption of data transmitted

Application Layers: These refer to the transactions and data relating to each computer-based application system and are therefore specific to each such application controls, which may be manual or programmed processing. Examples include data validation controls

ASP/MSP: A third party provider that delivers and manages applications and computer services, including security services to multiple users via the Internet or virtual private network

Asymmetric Key (Public Key): A cipher technique whereby different cryptographic keys are used to encrypt and decrypt a message

Asynchronous Transfer Mode (ATM): A is a high-bandwidth, low-delay switching and multiplexing technology. It is a data-link layer protocol. This means that it is a protocol-independent transport mechanism. ATM allows very high-speed data transfer rates at up to 155 Mbps

Audit Trail: A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source

Authentication: The act of verifying the identity of a system entity (user, system, or network node) and the entity's eligibility to access computerized information. Designed to protect against fraudulent log-on activity. Authentication also can refer to the verification of the correctness of a piece of data

Availability: Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities

Awareness: Cognizance, realization that, in this case, both threats and countermeasures exist and that our organization is not automatically immune or untargeted. This is the "what" and the "why" that drives our need for…

B

Baseband: A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver. In baseband, the entire bandwidth of the transmission medium (cable) is utilized for a single channel

Biometrics: A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint

Bit-stream Image: Bit-streams backups (also referred to as mirror image backups) involve all areas of a computer hard disk drive or another type of storage media. Such backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied

Brute Force: The name given to a class of algorithms that repeatedly try all possible combinations until a solution is found

Business Impact Analysis: An exercise that determines the effect of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum amount of resources needed to recover, and prioritizes the recovery of processes and supporting systems

C

Certificate Authority: A trusted third party that serves authentication infrastructures or organizations and registers entities and issues them certificates

Chain of Custody: The control over evidence. Lack of control over evidence can lead to it being discredited completely. Chain of custody depends on being able to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence so that it cannot in any way be changed and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering

Cipher: A type of algorithm used to encrypt data, changing plaintext into ciphertext and irreversible without a key

Ciphertext: Legible text in encrypted form, written in uppercase

Cleartext: Data that is not encrypted—plaintext

Cold Site: An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative computer facility

Confidentiality: Confidentiality concerns the protection of sensitive information from unauthorized disclosure

Criticality Analysis: An analysis or assessment of a business function or security vulnerability based on its criticality to the organization's business objectives. A variety of criticality may be used to illustrate the criticality

Cryptoanalysis: The art and science of breaking ciphers, decryption, through "unauthorized" means (unknown key)

Cryptography: The science of encrypting and decrypting messages, originating from the Greek terms *kryptos* (hidden) and *graphia* (writing)

Cryptology: The study of secure communications, formed from the Greek terms *kryptos* (hidden) and *logos* (word)

Cryptosystem: A system for encrypting information

Cybercops: A criminal investigator of online fraud or harassment

D

Data Classification: Data classification is assigning a level of sensitivity to data as they are being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled/secured and is also indicative of its value in terms of its importance to the organization

Data Diddling: Changing data with malicious intent before or during input to the system

Data Encryption Standard (DES): A private key cryptosystem published by the National Institutes of Standards and Technology. Data encryption standard has been used typically for data encryption in the forms of software and hardware implementation

Data Normalization: In data processing, this is a process applied to all data in a set that produces a specific statistical property. It is also the process of eliminating duplicate keys within a database. Useful because organizations use databases to evaluate various security data

Data Warehouse: A generic term for a system that stores, retrieves, and manages large amounts of data. Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches as well as advanced filtering

DDoS Attacks: Distributed denial-of-service attacks. These are denial-of-service assault from multiple sources

Decrypt: The process of unmasking the plaintext from the ciphertext. Also decipher

Decryption Key: A piece of information, in digitized form, used to recover the plaintext from the corresponding ciphertext by decryption

Defense-in-Depth: The practice of layering defenses to provide added protection. Security is increased by raising the cost to mount the attack. This system places multiple barriers between an attacker and an organization's business-critical information resources. This strategy also provides natural areas for the implementation of intrusion-detection technologies

Degauss: To have a device generate electric current (AC or DC) to produce magnetic fields for the purpose of reducing magnetic flux density to zero. A more secure means of destroying data on magnetic media

Digital Certificates: A certificate identifying a public key to its subscriber, corresponding to a private key held by that subscriber. It is a unique code that typically is used to allow the authenticity and integrity of communication to be verified

Digital Code Signing: The process of digitally signing computer code so that its integrity remains intact and it cannot be tampered with

Digital Signatures: A piece of information, a digitized form of signature, that provides sender authenticity, message integrity, and nonrepudiation. A digital signature is generated using the sender's private key or applying a one-way hash function

Disaster Notification Fees: The fee a recovery site vendor usually charges when the customer notifies them that a disaster has occurred and the recovery site is required. The fee is implemented to discourage false disaster notifications

Discretionary Access Control (DAC): A means of restricting access to objects based on the identity of subjects and groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to another subject

Disk Mirroring: This is the practice of duplicating data in separate volumes on two hard disks to make storage more fault-tolerant. Mirroring provides data protection in the case of disk failure, because data is constantly updated to both disks

DMZ: Often, it is the network segment between the Internet and a private network. It allows access to services from the Internet and the internal private network, while denying access from the Internet directly to the private network

Domain Name Service (DNS): A hierarchical database that is distributed across the Internet and allows names to be resolved to IP addresses and vice versa to locates services such as web and e-mail

Dual Control: A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource

Dynamic Host Configuration Protocol (DHCP): DHCP is an industry standard protocol used to dynamically assign IP addresses for network devices

E

Electronic Signature: Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures

Encrypt: The altering of plaintext using a keyword and specific algorithm so it becomes unintelligible to unauthorized parties, referred to as ciphertext. Also encipher

Enterprise Root: A certificate authority (CA) that grants itself a certificate and creates subordinate CAs. The root CA gives the subordinate CAs their certificates, but the subordinate CAs can grant certificates to users

Exposure: The potential loss to an area due to the occurrence of an adverse event

Extensible Markup Language (XML): A web-based application development technique that allows designers to create their own customized tags enabling the transmission, validation, and interpretation of data between application and organizations

F

Fall-through Logic: Predicting which way a program will branch when an option is presented. It is an optimized code based on a branch prediction

Firewall: A device that forms a barrier between a secure and an open environment. Usually, the open environment is considered hostile. The most notable open system is the Internet

Forensic Examination: After a security breach, the process of assessing, classifying, and collecting digital evidence to assist in prosecution. Standard crime scene standards are used

G

Guidelines: Documented suggestions for regular and consistent implementation of accepted practices. They usually have fewer enforcement powers

H

Honey-pots: A specifically configured server, designed to attract intruders so their actions do not affect production systems; also known as a decoy server

Hot Site: A fully operational offsite data-processing facility equipped with both hardware and system software to be used in the event of a disaster

Hypertext Transfer Protocol (HTTP): A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser

I

Information Security Governance: The management structure, organization, responsibility, and reporting processes surrounding a successful information security program

Information Security Program: The overall process of preserving confidentiality, integrity, and availability of information

Integrity: The accuracy, completeness, and validity of information in accordance with business values and expectations

Internet Engineering Task Force (IETF): The Internet standards setting organization with affiliates internationally from network industry representatives. This includes all network industry developers and researchers concerned with evolution and planned growth on the Internet

Internet Service Provider (ISP): A third party that provides organizations with a variety of Internet and Internet-related services

Intrusion Detection: The process of monitoring the events occurring on a computer system or network, detecting signs of security problems

Intrusion Detection System (IDS): An IDS inspects network traffic to identify suspicious patterns that may indicate a network or system attack from someone attempting to break in or compromise a system

IP Security Protocol (IPSec): A protocol in development by the IETF to support secure data exchange. Once completed, IPSec is expected to be widely deployed to implement virtual private networks. IPSec supports two encryption modes: transport and tunnel. Transport mode encrypts the data portion (payload) of each packet but leaves the header untouched. Tunnel mode is more secure because it encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet

ISO 17799: An international standard that defines information confidentiality, integrity, and availability controls

K

Key/Keyword: A word or system for encrypting or decrypting a cipher

M

Mail Relay Server: An e-mail server that relays messages where neither the sender nor the receiver is a local user. A risk exists that an unauthorized user could hijack these open relays and use them to spoof their own identity

Mandatory Access Control (MAC): MAC is a means of restricting access to data based on varying degrees of security requirements for information contained in the objects

Masqueraders: Attackers that penetrate systems by using user identifiers and passwords taken from legitimate users

Message Authentication Code: Message authentication code refers to an ANSI standard for a checksum that is computed with keyed hash that is based on a data encryption standard

Mirrored Site: An alternate site that contains the same information as the original. Mirror sites are set up for backup and DR as well to balance the traffic load for numerous download requests. Such "download mirrors" are often placed in different locations throughout the Internet

Mobile Site: The use of a mobile/temporary facility to serve as a business resumption location. They usually can be delivered to any site and can house information technology and staff

Monitoring Policy: The rules outlining the way in which information is captured and interpreted

N

Nonintrusive monitoring: The use on nonintrusive probes or traces to assemble information and track traffic and identity vulnerabilities

Nonrepudiation: The assurance that a party cannot later deny originating data. It is the provision of a proof of the integrity and origin of the data that can be verified by a third party. A digital signature can provide nonrepudiation

O

Offsite Storage: A storage facility located away from the building, housing the primary information processing facility (IPF), and used for storage of computer media such as offline backup data storage files

OSI 7-Layer Model: The Open System Interconnection seven-layer model is an ISO standard for worldwide communications that defines a framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy

P

Packet Filtering: Controlling access to a network analyzing the attributes of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules

Passive Response: A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action

Password Cracker: Specialized securities checker that tests user's passwords, searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries. Failing that, many password crackers can brute force all possible combinations in a relatively short time with current desktop computer hardware

Penetration Testing: A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers

Plaintext: The original, readable message, which is encrypted

Policy: A high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area

Ports: An interface point between the CPU and a peripheral device

Privacy: Freedom from unauthorized intrusion

Procedures: Are mandatory, step-by-step, detailed actions required to successfully complete a task

Proxy Server: A server that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user

Public Key: In an asymmetric cryptography scheme, the key that may be widely published to enable the operation of the scheme

R

Radius: Remote authentication dial in user service. A protocol used to authenticate remote users and wireless connections

Reciprocal Agreement: Emergency processing agreements between two or more organizations with similar equipment or applications. Typically, participants promise to provide processing time to each other when an emergency arises

Recovery Point Objective (RPO): A measurement of the point before an outage to which data are to be restored

Recovery Time Objective (RTO): The amount of time allowed for the recovery of a business function or resource after a disaster occurs

Redundant Site: A recovery strategy involving the duplication of key information technology components, including data, or other key business processes, whereby fast recovery can take place. The redundant site usually is located away from the original

Residual Risks: The risk associated with an event when the control is in place to reduce the effect or likelihood of that event being taken into account

Risk Assessment: A process used to identify and evaluate risks and their potential effects

Risk Avoidance: The process for systematically avoiding risk. Security awareness can lead to a better educated staff, which can lead to certain risks being avoided

Risk Mitigation: Although some risks cannot be avoided, they can be minimized or mitigated by putting controls into place to mitigate the risk once an incident occurs

Risk Transfer: The process of transferring risk. An example can include transferring the risk of a building fire to an insurance company

RSA: A public key cryptosystem developed by Rivest, Shamir, and Adleman. The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits. RSA is used for both encryption and digital signatures

S

Secure Socket Layer (SSL): A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection

Security Metrics: A standard of measurement used to measure and monitor information security–related activity

Sniffing: An attack capturing sensitive pieces of information, such as a password, passing through the network

Social Engineering: A person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords, and other confidential information

Split Knowledge: A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items. A condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module

Spoofing: Faking the sending address of a transmission to gain illegal entry into a secure system

Stand-alone Root: A certificate authority that signs its own certificates and does not rely of a directory service to authenticate users

Standards: A set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something. Standards are important because new technology will only take root once a group of specifications is agreed upon

Steering Committee: A management committee assembled to sponsor and manages various projects such as information security program

Steganography: A technology used to embed information in audio and graphical material. The audio and graphical materials appear unaltered until a steganography tool is used to reveal the hidden message

Symmetric Key Encryption: In symmetric key encryption, two trading partners share one or more secrets, no one else can read their messages. A different key (or set of keys) is needed for each pair of trading partners. The same key is used for encryption and decryption

T

TACACS+: Terminal Access Controller Access Control System Plus is an authentication protocol, often used by remote-access servers or single (reduced) sign-on implementations. TACACS and TACACS+ are proprietary protocols from CISCO

TCP/IP: Transmission Control Protocol/Internet Protocol is a set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access, and network management. TCP/IP provides the basis for the Internet

Threat Analysis: A project to identify the threats that exist over key information and information technology. The threat analysis usually also defines the level of the threat and likelihood of that threat to materialize

Two-Factor Authentication: The use of two independent mechanisms for authentication; for example, requiring a smart card and a password

V

Virtual Private Network (VPN): A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast with a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide area intranets. Using encryption and authentication, a VPN encrypts all data that passes between two Internet points, maintaining privacy and security

Virus Signature Files: A file of virus patterns that are compared with existing files to determine if they are infected with a virus. The vendor of the antivirus software updates the signatures frequently and makes them available to customers via the web

W

Warm Site: A warm site is similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery

Web Hosting: The business of providing the equipment and services required to host and maintain files for one or more web sites and to provide fast Internet connections to those sites. Most hosting is "shared," which means that web sites of multiple companies are on the same server to share costs

Web Server: Using the client–server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), Web Server is a software program that serves web page files to users

Worm: With respect to security, a special type of virus that does not attach itself to programs but rather spreads via other methods such as e-mail

Appendix A: Facilitated Risk Analysis and Assessment Process (FRAAP)

Company Information Security Analyst (ISA)	With the Company Owner, establish the Risk Assessment Scope statement and enter the approved statement in the appropriate location on the Risk Assessment Process Form (included at back of procedure)
	Provide the current Risk Assessment Threat Chart (included at back of procedure)
Company Owner (Unit or Department Director)	Using the Risk Assessment Threat Chart, identify how likely the threat is to occur during the next 12 months. Select the most appropriate of four choices: probable, moderate, rare, not applicable (see Likelihood Table for definitions). Enter the appropriate likelihood in the corresponding column adjacent to the threat in question. For those threats identified as not applicable, no further action is required
	Once all the threats have had a likelihood assigned, use the Impact Table to identify the severity level. There are three levels: high, medium, and low (see Impact Table for definitions). Enter the severity level in the corresponding column adjacent to the threat likelihood
	Using the Risk Matrix Table, find the point where the threat likelihood and the threat impact intersect. Enter the corresponding risk level in the appropriate column on the Threat Table. There are three risk levels: high, moderate, and low

Company Owner (Unit or Department Director)	Review the Notification Table to identify the Company management level that must be notified for the specific risk severity level
	After the form is completed and signed by the Division Director, submit the form to the Company Information Security Analyst (ISA)
ISA	In the appropriate column, enter the Division's Risk Assessment results into the Company Risk Assessment spreadsheet threat number tab
	Calculate the Company risk level by assigning the following values: high, 5; moderate, 4; low, 1; and not applicable, 0
	Enter the results in the risk score column next to the corresponding threat found in the threat number spreadsheet tab
	Copy the completed threat number tab into the risk score tab and sort the tab by the risk score column. This will rank the threats by risk severity. The risk score is typically divided into thirds. The upper third equates to high risk levels. Middle range scores equal moderate risk levels, and the lower third are the low risk levels
	For all high and moderate risk levels, create an action plan and enter the information into the action plan spreadsheet tab
	The cross-reference tab is completed by taking each proposed action and identifying all the risks that proposed action would mitigate
	Submit results to the Information Security Steering Committee (ISSC) for review and approval
ISSC	Review and approve or return for additional work (in either instance, the report is returned to the ISA)
ISA	If approved, implement risk assessment action mitigation plan
	If returned for more work, return to Company Division with recommendations for modifications

BRIA - 000			
Risk Assessment Process			
Company Division and Contributor Information			
Business Division		Date	
Division Director		Title	
Information Owner[a]		Phone	
Conducted by			
Other Contributors			

[a] Information Owner: the Director of the Division where the information is created, or who is the primary user of the information.

Risk Assessment Scope
The objective of performing risk assessment is to enable the Division to accomplish its mission(s) by better securing the systems and business processes that store, process, or transmit Company *restricted* or *confidential* information; by enabling Division Directors to make well-informed risk mitigation decisions to justify expenditures that are appropriate for the risk level identified, and by assisting management in authorizing access to the systems and information based on business need and least privilege
Likelihood—using the Threat Chart, identify how likely the threat is to occur during the next 12 months. Select the most appropriate of four choices: probable, moderate, rare, and not applicable (see page(s) 444 and 445). Enter the appropriate likelihood in the corresponding column adjacent to the threat in question. For those threats identified as not applicable, no more action is required
Impact—once all the threats have had a likelihood assigned, use the Impact Table to identify the severity level. There are three levels: high, medium, and low (see page 445). Enter the severity level in the corresponding column adjacent to the threat likelihood
Risk Level—using the Risk Matrix Table, find the point where the threat likelihood and threat impact meet. Enter the corresponding risk level in the appropriate column on the Threat Table. There are three risk levels: high, moderate, and low

Notification Table—review the Notification Table to identify the Company management level that must be notified for the specific risk severity level

Signatures

Division Director ______________________________ Date: __________________

Company ISA _________________________________ Date: __________________

Threat	*Likelihood*	*Impact*	*Risk Level*
Confidentiality			
E-mail could contain confidential and/or personally identifiable information (PII)			
Internal theft of information			
Employee is unable to verify the identity of a customer. Example: phone masquerading			
Confidential and/or PII may be left in plain view on a desk			
Social discussions outside the office could result in disclosure of confidential or PII			
Information could be salvaged from dumpsters, recycle bins, or other waste receptacles			
Information sent to third parties may not be properly secured			
Unattended computer could give unauthorized access to files			
Passwords may not be required for all workstations			
Mailing two or more different customer documents in one envelope			

Unauthorized people in restricted areas			
An undersecured work area could jeopardize the confidentiality of customer information			
Confidential or PII may be left on the fax or copy machine granting unauthorized viewing of documents			
Fraudulent or misrepresentation of individuals in phone conversations			
Employee could respond to a fax request without obtaining proper verification			
Documents sent out for customer signature could be forged and then returned			
Unauthorized access to information by viewing documents over the shoulder of an employee (shoulder surfing)			
Documents could be excessively duplicated			
Employee passwords could be shared			
Interoffice messengers may have access to confidential or PII			
Employee and messenger relationships could exchange sensitive or PII			
Rating	Probable Moderate Rare	High Medium Low	Use Matrix

Threat	*Likelihood*	*Impact*	*Risk Level*
Confidentiality			
Unauthorized disclosure of information by third parties			

Issues with third-party support requirements to fix problems could give access to confidential or PII			
Not adequately destroyed electronic media may leave confidential or PII available to unauthorized persons			
Actual customer information could be used on training templates causing disclosure of confidential or PII			
Employees may be overheard discussing confidential or PII outside the office			
Documents could be inadvertently delivered to wrong person			
Discussing confidential or PII loudly in office allowing others to hear details			
Use of the speakerphone may allow confidential or PII to be overheard			
Company could be subjected to electronic eavesdropping			
Terminated employees may be able to access the building, systems, or information			
Contract cleaning crews may have access to confidential or PII			
Trash could contain confidential or PII			
Temporary or new employees may be insufficiently trained			
Visitors may have access to restricted areas			
Information and files may be inappropriately accessed on company's systems			
Data stored off-site could be compromised			
Consultants or other contracted personnel may view confidential or PII			

Rating	Probable Moderate Rare	High Medium Low	Use Matrix

Threat	*Likelihood*	*Impact*	*Risk Level*
Integrity			
Faulty programming could (inadvertently) modify data			
Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons			
Data could be accidentally entered incorrectly			
Incorrect data could be intentionally entered			
Use of outdated programs could compromise integrity of information			
Faulty hardware could result in inaccurate data entry and analysis			
Third parties could modify data			
Files could be accidentally overlaid			
External hackers could change data			
Internal users could launch unauthorized programs to access and/or modify data			
Reports could be falsified			
Internal theft of information by employees could be modified and used later			
Network sniffing could intercept user passwords and allow unauthorized modification of information			

Outdated information could be used			
External hackers could obtain unauthorized access into the network to corrupt system resources			
Documents could be falsified to appear as official Company documents			
Unauthorized or fictitious sales could be approved			
Information could be misinterpreted due to language barriers			
Fraudulent programming could affect data integrity			
Computer viruses could modify data			
Information requests could be misdirected			
Rating	Probable Moderate Rare	High Medium Low	Use Matrix

Threat	*Likelihood*	*Impact*	*Risk Level*
Integrity			
Transactions could be intentionally not run or misrouted			
Newer or upgraded software could cause corruption of documents or files			
Incomplete or nonstandard procedures could cause misinterpretation of information			
Unauthorized persons may use an unattended workstation			
Information to and from third parties could be corrupted in transmission			
User account information (user ID/ password) may be shared			

A power failure could corrupt information			
Information could be submitted in a vague or misleading manner			
Someone could impersonate a customer to corrupt or falsify records			
Information could be taken outside the company			
Integrity of information could be compromised due to decay of information media			
Someone could impersonate an employee to corrupt or falsify information			
A terminated employee could intentionally corrupt information			
Company could be targeted for system hacking by a dissatisfied customer			
A default username and password for a network device could be exploited to gain access to system resources			
Rating	Probable Moderate Rare	High Medium Low	Use Matrix

Threat	*Likelihood*	*Impact*	*Risk Level*
Availability			
Files stored in personal directories may not be available to other employees when needed			
Hardware failures could affect the availability of company or department resources			
A failure in the data circuit could prohibit system access			
Act of God—flood or tornado could prevent access to company facilities and/or systems			
Upgrades in the software may affect system or data access			
Software upgrades could affect other programs			
Production system could be unavailable or down			
Spilling food or drink at a workstation could cause keyboard failure			
A power failure could interrupt employee access			
Expired user access could disrupt access to the computer system			
Insufficient employee training could disrupt access to the computer system			
Vendor or supplier support personnel may be unavailable to troubleshoot problems			
A communication failure could disrupt company operations			
Employees may have incorrect, inappropriate, or inadequate file access			

Sickness or other absence could render some critical files inaccessible			
A bomb threat could prevent access to the building			
Terrorist attack on local facilities could affect access to company system and information			
Theft of equipment or other information could affect ability to perform job assignments			
Insufficient cross-training of critical procedures could affect the company's mission			
Insufficient or missing desk procedures could affect department's ability to complete tasks			
Availability of information resources controlled by a third party could affect company processes			
Rating	Probable Moderate Rare	High Medium Low	Use Matrix

Threat	*Likelihood*	*Impact*	*Risk Level*
Availability			
Damaged or altered storage or hardware media could render systems or information unavailable			
Inadequate version control could cause back-level programs to be run			
Users could lose or misplace files			
Vandalism and sabotage could be attempted to the network			
Number of software licenses could be insufficient to meet requirements			

Insufficient personnel resources could affect business processes			
A malicious computer virus could be introduced via e-mail or removable media			
Denial of service attacks from malicious Internet users outside the company could render system or information inaccessible			
Employee could cause a document to be temporarily inaccessible due to human error			
A strike or protest could prevent access to the building			
Rating	Probable Moderate Rare	High Medium Low	Use Matrix

Company Likelihood Table	
Term	*Definition*
Likelihood	A measure of how likely a threat may occur during the next 12 months
Threshold Level	
Probable	Anticipated that the threat will occur one or more times during the next 12 months
Moderate	Possible that the threat may occur within the next 12 months
Rare	Highly unlikely that the threat will occur within the next 12 months

Not Applicable	Threat does not apply to this division's work process

Company Impact Table	
Term	*Definition*
Impact	The effect of a threat being carried out on the mission of the division under review
Severity Level	
High	An event with the potential to lead to permanent or long-term damage to the company's ability to achieve its mission
Medium	A significant event that can be managed under normal circumstances by the division
Low	An event where the consequences can be absorbed through normal activity

Risk Matrix			
	Impact		
Likelihood	*Low*	*Medium*	*High*
Probable	Moderate	High	High
Moderate	Low	Moderate	High
Rare	Low	Low	Moderate

Risk Action, Acceptance Level and Notification Table			
Risk Level	*Action*	*Acceptance Level*	*Notification Requirement*
High	Requires immediate corrective action	Executive Director	Company Executive Director
Moderate	Requires corrective action	Division Director	Division Director—possibly Company Executive Director
Low	Continue to monitor	Manager	Division Director

Appendix B: Business Impact Analysis

Kevin McLaughlin

The first order of business is to make sure that we know what systems are critical to maintaining an acceptable level of business service for our customers. The business impact analysis (BIA) is the critical component to understanding what services and what associated systems need to be restored as well as in what order and how quickly they need to be restored. Once organizational business management align on what items should be on the BIA (see Figure B.1), we then have a clear understanding of what services need to be restored and how quickly they need to be restored. To get business management alignment, the BIA process work needs to have an organizational sponsor who is high up enough in the organization to have authority over the business areas that are making the BIA decisions. This sponsor will assist with assuring that these decisions are made, will help negotiate any "tie-breaker" sessions where two services are seen as equal in criticality, and will ensure that business units engage in the BIA process as needed to develop the BIA outputs.

The sponsor will also help the business unit's work through the risk analysis that must take place when deciding whether or not to bring a system up quickly after an event. As Bergland and Pederson (1997, p. 291) stated in a report on the effects of safety regulation on the safety and well-being of Norwegian fisherman, costly regulation induced "the individual rational fisherman to behave in a way which increases their risks" of injury. This behavior is caused by a fundamental risk analysis being conducted on the part of the fisherman. Fishermen asked themselves if it will it cost them more to put safeguards in place than it will to suffer the accident or loss caused by a negative event. Extrapolating that risk analysis to the area of business continuity and DR planning, it is feasible to believe that senior business managers in other industries will conduct similar analyses. Will it cost me more to implement the required DR infrastructure than it would for me to recover from a

Application	Priority ranking (1–9)	Return to operation (time)	Acceptable data loss (days)	Comments
Access to critical systems AD/LDAP				Needed in order to access systems using User names and passwords. Also used by various applications to access systems
Basic web pages				Homepage with status event and recovery efforts
eMail				Basic email functionality
Finance				Payroll, loans, payments, etc.
Human resources				Employee processing, reporting, records management, etc.
Network services–enough to run the critical systems				Connects the systems and supporting systems together. Most applications will not work without a basic network in place
ERP system business data warehouse				Contains a multitude of data that is critical to organizational operations

Figure B.1 Example BIA template.

catastrophic event that may or may not occur sometime in the future? This is an impactful question that needs to be fully considered in our current economy downtrend that is causing organizations to pull back from IT spending.

The reality is that many organizations are simply too large to conduct a holistic BIA that incorporates feedback and discussion from every business unit that uses a service or part of a service and, therefore, the sponsor must also be in a position to speak for those units. Not every business unit needs direct involvement in the BIA hierarchal and rating discussions but they do need to have their voice heard. Indirectly, a BIA survey instrument can be sent to each and every organizational unit asking each person in the company to rank order a core set of services. This data can then be compiled and provided to the sponsor to assist them in their decision-making process and in speaking to the needs and viewpoint of the minor business units.

Once ready to start the ongoing BIA discussions, it is critical to host a kick-off meeting in which the process is explained, the sponsors provide their endorsement to getting the BIA completed, and their ongoing support to the overall organizational DR planning. During the BIA definition process, information about the following has to be gathered:

- What is the financial effect if the system is down and whether or not this financial effect increases the longer the system is down?
- Are there service level agreements (SLA) tied into this system and, if there is, what are the financial penalties incurred once the system is down past the agreed upon SLA timings?
- Are there manual workarounds for this service that are good enough?

- Is there a reputation or nontangible effect if the service is down for an extended period of time and is that effect one that will affect the survivability of the organization?
- What are all the systems and integration points between the systems that comprise this service and do they have time dependencies as to which system needs to be up before one of the other systems can work? Example: the e-Commerce systems are brought back online but if the network is still down, e-Commerce transactions are not going to take place.
- If this service goes down and we decide not to recover it in a quick time frame or consider it a critical system can (1) the business survive that decision or (2) can insurance be purchased to cover the financial effect suffered by a service being down until more critical systems are restored?

The overall goal of the BIA is to provide a very clear roadmap to the recovery team of the order that systems will be brought back online. Although a lot of work is being done in parallel and although good IT stewards are going to do their best to bring all the business systems up as quick as they can, it is critical to organizational survivability that the most critical systems are recovered first and that they get the attention from people and other resources that they need to recover in order of priority. It does not do the business any good to have BIA item no. 250 brought up before BIA item no. 1, and if key resources and personnel were used to bring up BIA item no. 250 when they could have helped with the quicker restoration of BIA item no. 1, then that should be seen as an organizational failure.

A typical BIA creation process should look like this: a key resource is identified to complete the BIA, the BIA sponsor(s) are identified, a survey is sent out to identify what are perceived to be the critical services, an information meeting is conducted (in person and virtually), the initial hierarchical list of services (according to the initial survey) is compiled, and interviews and meetings take place to establish rank order for the critical systems. It is important that transparency be maintained throughout the process and that what is thought to be the final rank order results are aligned across all the major business units involved in making the BIA ranking decisions. Lastly, the results should be shared with the sponsor who will make suggestions and decisions based on his knowledge of how impactful the listed services are to the organization. This review by the sponsor may lead to a revisit of the interviews and meetings that establish rank order for the services and this reiterative process between the business groups and sponsor may occur more than once before a final ranking is agreed upon. Figure B.2 depicts this process.

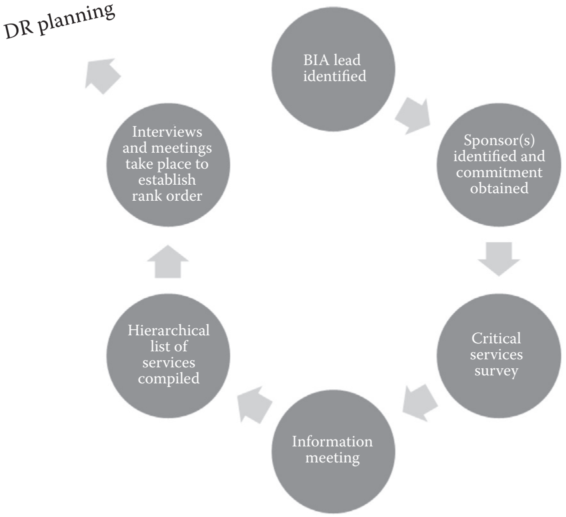

DR planning
BIA lead identified
Sponsor(s) identified and commitment obtained
Critical services survey
Information meeting
Hierarchical list of services compiled
Interviews and meetings take place to establish rank order

Figure B.2 DR planning.

Information Security Analyst	Provide Company Owner a list of business processes, systems, applications, and/or programs that have been identified as being "Owned" by that specific division
COMPANY Owner (Division Director)	Verify that business process list is complete and accurate
	Using the BIA Worksheet (see below), fill in the appropriate information. The worksheet is divided into three sections (header, activity period, and BIA score). The Criticality Table is also provided and used in step 6
	Fill in worksheet header with name of division, director, business process being analyzed, date of BIA, and who conducted BIA (if other than the Director)
	Using the activity period portion of the Impact Table, identify the business process activity periods. This could be normal, month-end, quarter-end, year-end, or some other time frame
	Using the Criticality Table as a guide, select the appropriate ranking level for each activity period as related to each business attribute (reputation, regulatory, customer, financial)

	Enter the numeric value for the criticality ranking level selected for each category on the BIA Impact Table in the proper column
	Once all appropriate impact values have been entered, multiply the impact values by the weight value and enter the product in the BIA Rating column
	When all of the multiplication products have been entered, add the total in each column and enter the sum in the Total Score box (the scores should range between a low of 4.5 and a high of 19.5)
	After the form is completed and signed by the Division Director, submit the form to the Company Information Security Project Analyst (ISA)
ISA	Enter the Division's BIA results into the company business process criticality log
	Submit results to Information Security Steering Committee (ISSC) for review and approval
ISSC	Review and approve or return for additional work (in either instance, the report is returned to ISPM)
ISA	If approved, update company business process criticality list
	If returned for more work, return to company division with recommendations for modifications

(4) BIA Worksheet			
Company Business Impact Analysis Worksheet			
Division Name	Formal Division Name	BIA date	Date BIA was conducted
Director Name	Director's name	Title	Director's formal title (for example, Executive Director)
Business Process Name	Application, system, program, business process, etc.	Phone	Director office phone number
BIA Conducted by	Name of person conducting the BIA		

(5) Activity Period				
	Use the BIA Criticality Table as a Guide to Identify the Ranking Level for Each Activity Period			
Identify Activity Periods	*Reputation*	*Regulatory*	*Customer*	*Financial*
Normal				
Peak 1 (e.g., month-end)				
Peak 2 (e.g., quarter-end)				
Peak 3 (e.g., year-end)				

(6) Criticality Table				
BIA Criticality Table				
Ranking level	Reputation	Regulatory	Customer	Financial
	Actual or potential effect on the reputation of Company in external environments. This includes the views held by all regulatory bodies that regulate any element of company's activities	Actual or potential effect arising from process failure, which leads to an inability to comply with laws, regulations, or policies and procedures	Actual or potential effect arising from process failure, which leads to an inability to provide service to our customer or execute against our business objectives	Actual or potential loss within any 12-month period

Urgent = 3	Likelihood of or actual adverse comment in any national media. Significantly affects our reputation on a national level	Likelihood of or actual disapproval by any of our regulators	Affecting more than 25% of our customers or employees. Total failure of a third-party service provider. Loss of a key system or failure to meet a business-critical process deadline. Will inhibit our ability to achieve our strategic objective. Management failure at an executive level	In excess of $10 million in a 12-month period
High = 2	Likelihood of or actual adverse comment in the local press or equivalent. Affects our reputation on a local level	Any event which may affect our standing with our regulators	Affecting between 5% and 25% of our customers or employees. Partial failure of a third-party service provider. Loss of a key system, which causes significant process or customer impact. Will delay our ability to achieve our strategic objectives. Management failure at a business division level	Between $2 million and $10 million in a 12-month period

Medium = 1	Any event that may tarnish our reputation with a specific customer, group, or third party	Minor regulatory issue requiring the oversight of internal resources	Affecting up to 5% of our customers or employees. Deteriorating performance of a third-party service provider. Loss of a key system that causes a minor process or customer impact. Management failure at a supervisory level	Between $200,000 and $2 million in a 12-month period

<table>
<tr><th colspan="7"><b>(7) BIA Impact Table</b></th></tr>
<tr><td colspan="7"><i>BIA Impact Table</i></td></tr>
<tr><td><i>Category</i></td><td><i>Impact Normal Period* U = 3, H = 2, M = 1</i></td><td><i>Weight</i></td><td><i>BIA Rating (Normal)</i></td><td><i>Impact Peak Period 1* U = 3, H = 2, M = 1</i></td><td><i>Weight</i></td><td><i>BIA Rating (Peak 1)</i></td></tr>
<tr><td>Reputation</td><td></td><td>2</td><td></td><td></td><td>2</td><td></td></tr>
<tr><td>Regulatory</td><td></td><td>2</td><td></td><td></td><td>2</td><td></td></tr>
<tr><td>Customer</td><td></td><td>1.5</td><td></td><td></td><td>1.5</td><td></td></tr>
<tr><td>Financial</td><td></td><td>1</td><td></td><td></td><td>1</td><td></td></tr>
<tr><td colspan="2">Impact × Weight = BIA Rating</td><td>Normal
Total Score:</td><td></td><td></td><td>Peak 1
Total Score:</td><td></td></tr>
</table>

BIA Impact Table						
Category	*Impact Peak Period 2* U = 3, H = 2, M = 1*	*Weight*	*BIA Rating (Peak 2)*	*Impact Peak Period 3* U = 3, H = 2, M = 1*	*Weight*	*BIA Rating (Peak 3)*
Reputation		2			2	
Regulatory		2			2	
Customer		1.5			1.5	
Financial		1			1	
Impact × Weight = BIA Rating		Peak 2 Total Score:			Peak 3 Total Score:	

Reference

Bergland, H. and Pedersen, P. Catch regulation and accident risk: the moral hazard of fisheries' management. *Marine Resource Economics* 12, 1997: 281–291.

Information Technology / Security & Auditing

Developing an information security program that adheres to the principle of security as a business enabler must be the first step in an enterprise's effort to build an effective security program. Following in the footsteps of its bestselling predecessor, ***Information Security Fundamentals, Second Edition*** provides information security professionals with a clear understanding of the fundamentals of security required to address the range of issues they will experience in the field.

The book examines the elements of computer security, employee roles and responsibilities, and common threats. It discusses the legal requirements that impact security policies, including Sarbanes-Oxley, HIPAA, and the Gramm-Leach-Bliley Act. Detailing physical security requirements and controls, this updated edition offers a sample physical security policy and includes a complete list of tasks and objectives that make up an effective information protection program.

- Includes ten new chapters
- Broadens its coverage of regulations to include FISMA, PCI compliance, and foreign requirements
- Expands its coverage of compliance and governance issues
- Adds discussions of ISO 27001, ITIL, COSO, COBIT, and other frameworks
- Presents new information on mobile security issues
- Reorganizes the contents around ISO 27002

The book discusses organization-wide policies, their documentation, and legal and business requirements. It explains policy format with a focus on global, topic-specific, and application-specific policies. Following a review of asset classification, it explores access control, the components of physical security, and the foundations and processes of risk analysis and risk management.

The text concludes by describing business continuity planning, preventive controls, recovery strategies, and how to conduct a business impact analysis. Each chapter in the book has been written by a different expert to ensure you gain the comprehensive understanding of what it takes to develop an effective information security program.

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K10531

ISBN: 978-1-4398-1062-0
90000
9 781439 810620

www.auerbach-publications.com